

# WebSphere Application Server Liberty

*Version 8 Release 5*



---

# Contents

## Chapter 1. Liberty overview . . . . . 1

Liberty: zero-migration architecture. . . . .	2
Java EE 7 in Liberty . . . . .	4
Liberty:Architecture . . . . .	6
Java EE 7 programming model support . . . . .	9
Java EE 6 programming model support . . . . .	13
Supported Java EE 6 and 7 feature combinations	16
Java EE 7 behavior changes . . . . .	17
Enterprise OSGi programming model support. . . . .	18
Liberty externals support. . . . .	19
Liberty:Server configuration . . . . .	21
Activation Specification (activationSpec). . . . .	22
Microsoft Active Directory LDAP Filters	
(activatedLdapFilterProperties) . . . . .	23
Administered Object (adminObject) . . . . .	24
Administrator Role (administrator-role) . . . . .	24
API Discovery (apiDiscovery) . . . . .	24
Application (application) . . . . .	25
Application Manager (applicationManager). . . . .	37
Application Monitoring (applicationMonitor) . . . . .	38
z/OS Connect SMF Audit Interceptor	
(auditInterceptor) . . . . .	39
Authentication Cache (authCache). . . . .	39
Authentication Data (authData). . . . .	39
Authentication Filter (authFilter) . . . . .	40
Authentication (authentication) . . . . .	42
Feature Authorization Role Mapping	
(authorization-roles) . . . . .	42
z/OS Connect Authorization Interceptor	
(authorizationInterceptor). . . . .	43
Basic User Registry (basicRegistry) . . . . .	44
Batch JMS Dispatcher (batchJmsDispatcher) . . . . .	45
Batch JMS Events (batchJmsEvents) . . . . .	62
Batch JMS Executor (batchJmsExecutor) . . . . .	74
Batch Job Logging (batchJobLogging) . . . . .	103
Batch Persistence (batchPersistence) . . . . .	103
BELL (bell) . . . . .	155
OSGi Applications Bundle Repository	
(bundleRepository) . . . . .	157
Contexts And Dependency Injection (CDI) V1.2	
(cdi12). . . . .	158
CDI Container (cdiContainer) . . . . .	158
Channel Framework (channelfw) . . . . .	158
Classloading (classloading) . . . . .	159
Cloudant Builder (cloudant) . . . . .	159
Cloudant Database (cloudantDatabase) . . . . .	165
Cluster Member (clusterMember). . . . .	171
WebSphere Cluster Manager	
(clusterPluginConfig) . . . . .	171
Certificate Authority Signed Certificate	
(collectiveCertificate) . . . . .	171
Collective Controller (collectiveController). . . . .	172
Collective Member (collectiveMember) . . . . .	173
WebSphere Collective Repository MBean	
(collectiveRepository). . . . .	174
Configuration Management (config) . . . . .	174

Connection Factory (connectionFactory) . . . . .	176
Connection Manager (connectionManager) . . . . .	180
Thread Context Propagation (contextService) . . . . .	182
Cross-Origin Resource Sharing (cors) . . . . .	186
CouchDB (couchdb) . . . . .	187
Custom LDAP Filters	
(customLdapFilterProperties) . . . . .	190
Data Source (dataSource) . . . . .	191
Database Store (databaseStore) . . . . .	240
DeployManager (deployManager) . . . . .	291
Deploy Rule (deployRule) . . . . .	291
DeployVariable (deployVariable) . . . . .	292
Distributed Map (distributedMap) . . . . .	292
SIP Domain Resolver (domainResolver) . . . . .	296
IBM Lotus Domino LDAP Filters	
(domino50LdapFilterProperties) . . . . .	297
Dynamic Routing (dynamicRouting). . . . .	298
Novell eDirectory LDAP Filters	
(edirectoryLdapFilterProperties) . . . . .	301
EJB Application (ejbApplication) . . . . .	301
EJB Container (ejbContainer) . . . . .	308
Enterprise Application (enterpriseApplication) . . . . .	322
Event Logging (eventLogging). . . . .	335
Executor Management (executor) . . . . .	336
Feature Manager (featureManager) . . . . .	339
User Registry Federation (federatedRepository) . . . . .	339
z/OS Connect File System Logger Interceptor	
(fileSystemloggerInterceptor) . . . . .	349
Fileset (fileset) . . . . .	350
Health Policy (healthPolicy) . . . . .	351
Host Access (hostAccess) . . . . .	354
Host Authentication Information (hostAuthInfo) . . . . .	355
Host Singleton (hostSingleton). . . . .	357
HTTP Access Logging (httpAccessLogging) . . . . .	357
HTTP Dispatcher (httpDispatcher) . . . . .	358
HTTP Transport Encoding (httpEncoding) . . . . .	358
HTTP Endpoint (httpEndpoint) . . . . .	361
HTTP Options (httpOptions) . . . . .	366
HTTP Proxy Redirect (httpProxyRedirect) . . . . .	367
HTTP Session (httpSession). . . . .	368
HTTP Session Database (httpSessionDatabase) . . . . .	373
HTTP Whiteboard (httpWhiteboard). . . . .	379
IBM Tivoli Directory Server LDAP Filters	
(idsLdapFilterProperties) . . . . .	380
IIOP Endpoint (iiopEndpoint) . . . . .	380
IIOP Server Policies (iiopServerPolicies) . . . . .	382
Include (include) . . . . .	382
Installable (installable) . . . . .	383
Sun Java System Directory Server LDAP Filters	
(iplanetLdapFilterProperties) . . . . .	383
JAAS Login Context Entry	
(jaasLoginContextEntry) . . . . .	384
JAAS Login Module (jaasLoginModule) . . . . .	384
Java 2 Security (javaPermission) . . . . .	387
JDBC Driver (jdbcDriver) . . . . .	388
JMS Activation Specification (jmsActivationSpec) . . . . .	390

JMS Connection Factory (jmsConnectionFactory)	403	SAML Web SSO 2.0 Authentication (samlWebSso20)	682
JMS Destination (jmsDestination)	415	Scaling Definitions (scalingDefinitions)	692
JMS Queue (jmsQueue)	415	Scaling Member (scalingMember)	698
JMS Queue Connection Factory (jmsQueueConnectionFactory)	419	IBM SecureWay Directory Server LDAP Filters (securewayLdapFilterProperties)	699
JMS Topic (jmsTopic)	429	Server Commands MBean (serverCommands)	699
JMS Topic Connection Factory (jmsTopicConnectionFactory)	433	SIP Application Router (sipApplicationRouter)	700
JNDI Entry (jndiEntry)	445	SIP Container (sipContainer)	700
JNDI Object Factory (jndiObjectFactory)	445	SIP Endpoint (sipEndpoint)	702
JNDI Reference Entry (jndiReferenceEntry)	447	SIP Stack (sipStack)	704
JNDI URL Entry (jndiURLEntry)	449	Spnego Authentication (spnego)	710
JPA Container (jpa)	450	SSL Repertoire (ssl)	713
JSP Engine (jspEngine)	451	SSL Default Repertoire (sslDefault)	715
Keystore (keyStore)	452	SSL Options (sslOptions)	715
LDAP User Registry (ldapRegistry)	454	Stack Group (stackGroup)	716
Shared Library (library)	466	Stack Manager (stackManager)	718
WebSphere Optimized Local Adapters (WOLA) Connect (localAdaptersConnectService)	468	Sync-to-OS-thread (syncToOSThread)	719
Logging (logging)	472	TCP Options (tcpOptions)	719
Logstash Collector (logstashCollector)	474	Timed Operation (timedOperation)	721
LTPA Token (ltpa)	475	Transaction Manager (transaction)	722
Mail Session Object (mailSession)	475	Trust Association Interceptor (trustAssociation)	775
Managed Executor (managedExecutorService)	476	User Information (userInfo)	777
Managed Scheduled Executor (managedScheduledExecutorService)	480	Variable Declaration (variable)	778
Managed Thread Factory (managedThreadFactory)	485	Virtual Host (virtualHost)	778
Messaging Engine (messagingEngine)	490	WAS JMS Endpoint (wasJmsEndpoint)	782
Default Mime Types (mimeTypes)	496	WAS JMS Outbound (wasJmsOutbound)	784
Mongo (mongo)	496	Web Container Application Security (webAppSecurity)	786
MongoDB DB (mongoDB)	501	Web Application (webApplication)	790
Monitor (monitor)	507	Web Container (webContainer)	797
RRS Native Transaction Manager (nativeTransactionManager)	508	WLM Classification (wlmClassification)	802
Netscape Directory Server LDAP Filters (netscapeLdapFilterProperties)	508	WebSphere MQ Messaging (wmqJmsClient)	803
OAuth Role Map (oauth-roles)	509	WS-AtomicTransaction (wsAtomicTransaction)	804
OAuth Provider Definition (oauthProvider)	511	WS-Security Client (wsSecurityClient)	805
OpenId Authentication (openId)	570	WS-Security Provider (wsSecurityProvider)	806
OpenID Connect Client (openidConnectClient)	574	WAS WebSocket Outbound (wsocOutbound)	810
OpenID Connect Server Provider (openidConnectProvider)	580	z/OS Connect Data Transformer (zosConnectDataXform)	813
Object Request Broker (ORB) (orb)	644	z/OS Connect Interceptors (zosConnectInterceptors)	814
OSGi Application (osgiApplication)	650	z/OS Connect Manager (zosConnectManager)	814
OSGi Applications (osgiApplications)	653	z/OS Connect Endpoint (zosConnectService)	817
OSGi Library (osgiLibrary)	653	z/OS Connect REST Client (zosConnectServiceRestClient)	821
Package (package)	655	z/OS Connect Rest Client Basic Authentication (zosConnectServiceRestClientBasicAuth)	823
Persistent Scheduled Executor (persistentExecutor)	655	WOLA (zosLocalAdapters)	823
Web Server Plugin (pluginConfiguration)	661	z/OS Logging (zosLogging)	824
Quick Start Security (quickStartSecurity)	669	WLM Native Enclave Manager (zosWorkloadManager)	824
Remote File Access (remoteFileAccess)	669	Liberty: Feature management	824
Request Timing (requestTiming)	670	Liberty features	826
Resource Adapter (resourceAdapter)	670	Liberty Kernel	964
Real-Time Communications (rtcomm)	676	Liberty: Liberty Repository	965
SAF Authorization (safAuthorization)	680	Liberty profile: Product extension	967
SAF Credentials (safCredentials)	681	Liberty: Security	971
SAF User Registry (safRegistry)	682	Liberty:Quick overview of security	975
SAF Role Mapper (safRoleMapper)	682	Liberty:Authentication	976
		Liberty: Authorization	999

Security on the Liberty application client container . . . . .	1001
Liberty: Java 2 Security . . . . .	1002
Liberty:Security public APIs . . . . .	1004
Configuration differences between the traditional and Liberty: security . . . . .	1008
Liberty:The limits to protection through password encryption . . . . .	1009
Liberty:JMS messaging . . . . .	1010
Liberty JMS messaging providers . . . . .	1010
JMS messaging (wasJmsClient-2.0) behavior changes . . . . .	1014
Java Persistence API (JPA). . . . .	1015
Java Persistence API (JPA) feature overview	1016
Java Persistence API 2.1 behavior changes . . . . .	1017
Liberty profile: Process types on z/OS . . . . .	1019
IBM z/OS Connect overview . . . . .	1020
Liberty:Binary logging . . . . .	1023
BinaryLog command options . . . . .	1027
Configuring binary logging in Liberty . . . . .	1031
Liberty: Session Initiation Protocol (SIP) . . . . .	1033
Session Initiation Protocol (SIP) applications on Liberty . . . . .	1033
Session Initiation Protocol (SIP) container on Liberty . . . . .	1035
SIP industry standards compliance on Liberty	1035
Liberty: Real-Time Communications . . . . .	1038
Configuring Liberty Real-Time Communications . . . . .	1039
Using the rtcomm-1.0 WebRTC JavaScript client and services . . . . .	1042
Configuring a Rtcomm Gateway . . . . .	1042
Configuring Security for the rtcomm-1.0 Feature . . . . .	1044
Configuring the Media Server Control Feature	1046
Multimedia . . . . .	1046
Video: Comparing collectives and cells . . . . .	1047
Video: Configure session cache management with Liberty and WebSphere eXtreme Scale . . . . .	1049
Video: Configuring a Liberty auto-scalable cluster for JVM elasticity . . . . .	1055
Video: Configuring an auto-scalable cluster for Liberty elasticity . . . . .	1059
Video: DevOps with WebSphere Liberty Server	1069
Video: Enabling IHS for Liberty Dynamic Routing . . . . .	1074
Video: Getting started with the Server Configuration Tool for WebSphere Liberty . . . . .	1078
Video: Google OpenID Connect for applications on WebSphere Liberty . . . . .	1079
Video: Health management for Liberty collectives . . . . .	1084
Video: Installing Liberty from a ZIP file . . . . .	1086
Video: Introduction to creating a collective	1088
Video: Java EE 7 in Liberty . . . . .	1092
Video: OpenID Connect on Liberty . . . . .	1098
Video: Setting up Admin Center . . . . .	1104
Video: Thoughts on Liberty: Interview with Alasdair Nottingham . . . . .	1106
Video: Touring Admin Center . . . . .	1107

Video: Using the IBM WebSphere Liberty Repository to enhance Liberty environments . . . . .	1108
Video: Why Liberty? Performance that scales	1110
Video: Why Liberty? Fast application development . . . . .	1113
Video: Why Liberty? Rapid deployment and powerful administration . . . . .	1114
Notices . . . . .	1116
Privacy Policy Considerations . . . . .	1119

## Chapter 2. End-to-end paths for Liberty . . . . . 1121

Enabling JMS messaging for Liberty . . . . .	1121
Enabling JMS messaging for a single Liberty server . . . . .	1122
Enabling JMS messaging between two Liberty servers . . . . .	1124
Enabling secure JMS messaging for Liberty	1126
Enabling interoperability between Liberty and WebSphere Application Server traditional . . . . .	1130
Configuring connection pooling for JMS connections . . . . .	1132
Securing JMS communications in Liberty by using SSL . . . . .	1133
Setting up the server-management environment for Liberty by using collectives . . . . .	1134
Configuring a Liberty collective . . . . .	1136
Registering host computers with a Liberty collective . . . . .	1142
Overriding Liberty server host information	1144
Setting the JAVA_HOME variable for Liberty collective members . . . . .	1147
Configuring Liberty collective replica sets . . . . .	1148
Setting up Liberty server clusters . . . . .	1153

## Chapter 3. Migrating applications to Liberty . . . . . 1157

Migrating data access applications to Liberty . . . . .	1157
Configuration differences between the traditional and Liberty: dataSource and jdbcDriver elements . . . . .	1157
Configuration differences between the traditional and Liberty: connectionManager element . . . . .	1158
Migrating a DB2 data source to Liberty . . . . .	1159
Migrating a Derby embedded data source to Liberty . . . . .	1161

## Chapter 4. Installing Liberty . . . . . 1163

Installing and uninstalling Liberty using Installation Manager . . . . .	1164
Installing and uninstalling Liberty on distributed operating systems . . . . .	1165
Installing and uninstalling Liberty on IBM i operating systems . . . . .	1292
Installing Liberty on z/OS . . . . .	1343
Installing and uninstalling Liberty using downloaded files and archives . . . . .	1371
Installing Liberty developer tools and (optionally) Liberty . . . . .	1374

Installing Liberty by extracting a Java archive file . . . . .	1374
Installing Liberty by extracting a ZIP archive file . . . . .	1381
Upgrading Liberty installations . . . . .	1386
Applying an interim fix to a Liberty archive installation . . . . .	1388
Configuring the Liberty server to start as a job in the QWAS85 subsystem on IBM i . . . . .	1390
Uninstalling Liberty application-serving environment from IBM i operating systems . . . . .	1390
Installing Liberty Repository assets . . . . .	1391
Installing assets using the installUtility command . . . . .	1393
Installing assets using the featureManager command . . . . .	1403
Installing assets using Installation Manager . . . . .	1411
Installing assets by using developer tools . . . . .	1413
Verifying the integrity of Liberty installation . . . . .	1414
Liberty:productInfo command . . . . .	1415
Docker support in Liberty . . . . .	1416
Accessing a remote Liberty server in a Docker container by using developer tools . . . . .	1417
Liberty and Chef . . . . .	1418
Installing the OpenShift Cartridge for Liberty . . . . .	1418
Installing the IBM WebSphere Application Server Liberty Buildpack into a Cloud Foundry Environment . . . . .	1420
Structure a Liberty repository for personal binary files . . . . .	1421
<b>Chapter 5. Setting up Liberty . . . . .</b>	<b>1423</b>
Creating a Liberty server manually . . . . .	1423
Creating a Liberty server by using developer tools . . . . .	1424
Creating a remote Liberty server by using developer tools . . . . .	1427
Creating a workbench Liberty server in a Docker container by using developer tools . . . . .	1430
Liberty:Directory locations and properties . . . . .	1434
Specifying Liberty bootstrap properties . . . . .	1437
Setting the default host name of a Liberty server . . . . .	1439
Liberty: Default port numbers . . . . .	1440
Using virtual hosts . . . . .	1441
Isolating two applications from each other . . . . .	1441
Isolating applications based on the requested host or port . . . . .	1442
Restricting access based on originating endpoint . . . . .	1442
Virtual hosts . . . . .	1443
Preparing and running an application client . . . . .	1445
Creating a Liberty application client manually . . . . .	1446
Creating a Liberty application client with multiple client modules . . . . .	1447
Setting up the server-management environment for Liberty by using collectives . . . . .	1448
Liberty: Collective architecture . . . . .	1450
Liberty: Collective security . . . . .	1453
Configuring a Liberty collective . . . . .	1454
Overriding Liberty server host information . . . . .	1461
Starting and stopping a Liberty collective member . . . . .	1463

Registering host computers with a Liberty collective . . . . .	1464
Configuring Liberty collective replica sets . . . . .	1467
Generating collective controller SSL keys . . . . .	1475
Setting administrative metadata for Liberty resources . . . . .	1476
Updating a Liberty collective . . . . .	1480
Setting up Liberty server clusters . . . . .	1485
Setting the JAVA_HOME variable for Liberty collective members . . . . .	1490
Setting up RXA for Liberty collective operations . . . . .	1491
Setting up dynamic routing for Liberty collectives . . . . .	1493
Setting up auto scaling for Liberty collectives . . . . .	1503
Entering maintenance mode for Liberty collectives . . . . .	1516
Configuring health management for Liberty Liberty collective troubleshooting . . . . .	1519
Setting up a Liberty server to use Bluemix services . . . . .	1529
bluemixUtility command . . . . .	1529
Configuring Liberty for Bluemix Cloudant services . . . . .	1533
Configuring Liberty for Bluemix Watson services . . . . .	1535
Setting up a Liberty Server for use with z/OS Connect . . . . .	1536
Setting up z/OS Connect . . . . .	1536
Defining z/OS Connect services . . . . .	1537
Setting up the z/OS Connect REST client service . . . . .	1541
Defining z/OS Connect interceptors . . . . .	1542
Setting up the z/OS Connect file system logger interceptor . . . . .	1544
Defining z/OS Connect message payload transformations . . . . .	1545
Auditing and tracking with z/OS Connect . . . . .	1548
z/OS Connect high availability . . . . .	1550
Configuring security for z/OS Connect . . . . .	1550
Platform-as-a-service environment considerations for setting up Liberty . . . . .	1553
<b>Chapter 6. Administering Liberty . . . . .</b>	<b>1555</b>
XML escape characters . . . . .	1555
Administering Liberty by using developer tools . . . . .	1556
Editing the Liberty configuration by using developer tools . . . . .	1556
Specifying the Liberty configuration with dropins files by using developer tools . . . . .	1557
Starting and stopping a server by using developer tools . . . . .	1558
Switching a Liberty Docker server between run and debug mode by using developer tools . . . . .	1558
Defining a utility project as a shared library . . . . .	1559
Exploring the runtime environment by using developer tools . . . . .	1561
Displaying the server configuration in a merged view . . . . .	1562
Viewing the schema documentation for the server configuration . . . . .	1563

Generating a Liberty server dump using developer tools . . . . .	1563
Packaging a Liberty server by using developer tools . . . . .	1563
Adding a data source by using developer tools	1564
Administering Liberty manually. . . . .	1564
Customizing the Liberty environment . . . . .	1565
Administering Liberty from the command line	1567
Adding and removing Liberty features . . . . .	1587
Using include elements, variables, and Ref tags in configuration files . . . . .	1588
Controlling dynamic updates. . . . .	1594
Configuring class loaders and libraries for Java EE applications . . . . .	1596
Configuring libraries for OSGi applications	1600
Configuring JPA for Liberty . . . . .	1601
Configuring a web server plug-in for Liberty	1604
Configuring session persistence for Liberty	1610
Configuring and deploying a basic JCA ResourceAdapter . . . . .	1612
Configuring ManagedExecutorService instances	1633
Configuring thread context service instances	1635
Configuring managed scheduled executors	1637
Configuring managed thread factories. . . . .	1639
Connecting to Liberty by using JMX . . . . .	1641
Establishing a JMX MBean Liberty server connection . . . . .	1658
Liberty: File transfer. . . . .	1660
Transferring files in a Liberty collective . . . . .	1660
Configuring binary logging in Liberty. . . . .	1667
Administering the transaction service on Liberty . . . . .	1668
Administering data access resources on Liberty	1672
Administering web applications on Liberty	1712
Administering Contexts and Dependency Injection applications on Liberty. . . . .	1725
Administering Session Initiation Protocol (SIP) on Liberty . . . . .	1728
Administering JavaMail on Liberty. . . . .	1730
Administering Liberty on z/OS . . . . .	1731
Administering Liberty using Admin Center . . . . .	1741
Setting up Admin Center . . . . .	1742
Logging in to Admin Center . . . . .	1745
Customizing the Toolbox . . . . .	1746
Editing server configuration files in Admin Center . . . . .	1748
Exploring and managing resources with Admin Center . . . . .	1749
Deploying resources with Admin Center . . . . .	1761
Monitoring background tasks . . . . .	1764
Configuration updates . . . . .	1766
Liberty and Chef . . . . .	1767
Liberty:Including configuration information from external xml files in the server.xml file . . . . .	1767
Liberty:Configuration element merging rules . . . . .	1768

## Chapter 7. Extending Liberty . . . . 1771

Developing a Liberty feature for Liberty . . . . .	1771
Developing a Liberty feature manually . . . . .	1771
Creating a Liberty feature by using developer tools . . . . .	1782

Developing an OSGi bundle with simple activation . . . . .	1788
Composing advanced features by using OSGi Declarative Services . . . . .	1793
Advanced Configuration . . . . .	1798
Providing an application endpoint . . . . .	1808
Liberty SPI utilities . . . . .	1808
Including protected features . . . . .	1816
Locating OSGi applications . . . . .	1818
Developing with the JNDI default namespace in a Liberty feature . . . . .	1819
Developing a custom TAI as a Liberty feature	1820
Dynamic content management . . . . .	1821
Packaging and installing Liberty features. . . . .	1822
Provide product information for your feature extension . . . . .	1823
Embedding Liberty in your applications . . . . .	1824
Creating Liberty servers from custom configurations. . . . .	1826
Disabling z/OS operator console command handling in the Liberty server . . . . .	1826

## Chapter 8. Securing Liberty and its applications . . . . . 1829

Getting started with security in Liberty . . . . .	1829
Liberty:Quick overview of security . . . . .	1831
Setting up BasicRegistry and role mapping on Liberty . . . . .	1832
Securing communications in Liberty . . . . .	1833
Enabling SSL communication in Liberty . . . . .	1834
Creating SSL certificates for your Liberty using the Utilities menu . . . . .	1844
Creating SSL certificates from the command line . . . . .	1844
Configuring your web application and server for client certificate authentication . . . . .	1847
Setting up Liberty to run in SP800-131a . . . . .	1848
Configuring an httpEndpoint to use an SSL configuration other than the default . . . . .	1850
Authenticating users in Liberty . . . . .	1850
Configuring a user registry for Liberty . . . . .	1851
Configuring the authentication cache in Liberty	1867
Configuring a JAAS custom login module for Liberty . . . . .	1868
Configuring a Java Authentication SPI for Containers (JASPIC) User Feature . . . . .	1871
Configuring LTPA in Liberty . . . . .	1872
OpenID . . . . .	1873
OpenID Connect . . . . .	1875
Configuring an OpenID Relying Party in Liberty . . . . .	1878
Configuring SPNEGO authentication in Liberty	1879
Customizing SSO configuration using LTPA cookies in Liberty . . . . .	1887
Configuring RunAs authentication in Liberty	1888
Configuring TAI in Liberty . . . . .	1889
Configuring a custom form login page . . . . .	1891
Configuring SAML Web Browser SSO in Liberty . . . . .	1893
Using OpenID Connect. . . . .	1897
Authentication Filters . . . . .	1937

Authorizing access to resources in Liberty . . . . .	1939
Configuring authorization for applications in Liberty . . . . .	1939
Enabling z/OS authorized services in Liberty for z/OS . . . . .	1942
Configuring distributed identity filters in z/OS security . . . . .	1948
Securing optimized local adapters on Liberty for z/OS . . . . .	1949
Configuring security authorization for Liberty servers on IBM i . . . . .	1952
OAuth . . . . .	1953
Configuring Common Secure Interoperability version 2 (CSIv2) in Liberty . . . . .	1973
Configuring inbound CSIv2 in Liberty . . . . .	1974
Configuring outbound CSIv2 in Liberty . . . . .	1979
Configuring security for the Liberty application client container and its applications . . . . .	1984
Enabling SSL communication for the Liberty application client container . . . . .	1984
Configuring a JAAS programmatic login on the Liberty application client container . . . . .	1986
Configuring a JAAS custom login module for the Liberty application client container . . . . .	1988
Configuring Common Secure Interoperability version 2 (CSIv2) in the Liberty application client container . . . . .	1989
Configuring Java Servlet 3.1 support for security	1991
Configuring secure JMX connection to Liberty	1993
Configuring web security related properties in Liberty . . . . .	1994
Customizing SSO configuration using LTPA cookies in Liberty . . . . .	1994
Configuring your web application and server for client certificate authentication . . . . .	1995
Configuring the Liberty server to track logged out LTPA tokens . . . . .	1996
Configuring authentication aliases for Liberty	1997
Configuring JAAS for database authentication	1997
Developing extensions to the Liberty security infrastructure . . . . .	1998
Developing a custom TAI for Liberty . . . . .	1998
Developing JAAS custom login modules for a system login configuration . . . . .	2002
Developing a custom JASPIC authentication provider for Liberty . . . . .	2006
Developing a Java Authorization Contract for Containers (JACC) Authorization Provider . . . . .	2009
Developing a customPasswordEncryption Provider . . . . .	2011
Customizing an application login to perform an identity assertion by using JAAS . . . . .	2013
Developing a custom user registry in Liberty	2014
Developing JAAS custom login modules for database authentication . . . . .	2015
Developing a programmatic login for obtaining authentication data . . . . .	2016
Developing a custom thread identity service	2017
Web services security . . . . .	2018
Securing web services at the transport level	2018
Web Services Security at the message level	2027

Web Services Security HTTPS transport policy assertions . . . . .	2069
Liberty:Security considerations . . . . .	2070
Securing Liberty by using HTTP Strict Transport Security (HSTS) . . . . .	2071

## Chapter 9. Developing applications in the Liberty environment . . . . . 2073

Developing applications that interact with z/OS resources . . . . .	2073
Developing applications that use optimized local adapters on Liberty . . . . .	2073
Developing applications for use with z/OS Connect to reach z/OS assets. . . . .	2105
Developing EJB applications on Liberty . . . . .	2116
Developing Enterprise bean (EJB) persistent timer applications . . . . .	2117
Using enterprise JavaBeans with remote interfaces on Liberty . . . . .	2122
Using enterprise JavaBeans applications that call local EJB components in another application . . . . .	2125
Developing SIP applications on Liberty . . . . .	2125
Developing SIP applications that support PRACK on the Liberty . . . . .	2126
Developing back-to-back (B2B) applications	2127
Developing applications that use the Asynchronous Invocation API on the Liberty profile . . . . .	2128
Performing DNS lookups in Session Initiation Protocol (SIP) applications on the Liberty profile . . . . .	2131
Receiving unmatched messages in Session Initiation Protocol (SIP) on Liberty . . . . .	2131
SIP proprietary header fields on Liberty . . . . .	2132
SIP SipServletRequest and SipServletResponse classes on Liberty . . . . .	2133
SIP SipSession and SipApplicationSession classes on Liberty . . . . .	2134
Developing OSGi applications in Liberty . . . . .	2134
Enable OSGi Applications with Java EE 7 technologies . . . . .	2134
Enabling integration of OSGi application services . . . . .	2135
Custom blueprint namespace handlers . . . . .	2136
Developing WebSocket applications in Liberty	2137
WebSocket . . . . .	2138

## Chapter 10. Deploying applications in Liberty. . . . . 2139

Adding and running an application on Liberty by using developer tools . . . . .	2141
Publishing your application by using developer tools . . . . .	2142
Restart requirements for a modified application on Liberty . . . . .	2143
Customizing automatic feature detection . . . . .	2144
Packaging a Liberty server from the command line . . . . .	2144

Using JNDI binding for constants from the server configuration files . . . . .	2146
Using JNDI binding for dynamic values from the server configuration files . . . . .	2148
Deploying OSGi applications to Liberty . . . . .	2149
Sharing common OSGi bundles for Liberty	2149
Deploying data access applications to Liberty	2149
Deploying an existing JDBC application to Liberty . . . . .	2150
Enabling JDBC Tracing for Liberty . . . . .	2152
Deploying a web application to Liberty . . . . .	2155
Deploying SIP applications to Liberty . . . . .	2156
Deploying a JPA application to Liberty . . . . .	2157
Liberty:Enhancement of JPA entities for JPA 2.0	2158
Deploying web services applications to Liberty	2158
Deploying JAX-RS 2.0 applications to Liberty	2159
Deploying JAX-WS applications to Liberty	2178
Deploying messaging applications to Liberty . . . . .	2195
Deploying JMS applications to connect to the embedded messaging server . . . . .	2195
Deploying JMS applications to Liberty to use the IBM MQ messaging provider . . . . .	2197
Deploying JMS application to connect to the Service Integration Bus running on WebSphere Application Server traditional . . . . .	2198
Deploying JMS applications on the Liberty application client container . . . . .	2199
Enabling JMS tracing for the Liberty embedded messaging . . . . .	2200
Deploying message-driven beans within Liberty . . . . .	2201
Configuring connection pooling for JMS connections. . . . .	2207
Deploying Java batch applications for Liberty	2208
Java batch and managed batch overview . . . . .	2208
Configuring Liberty for the batch REST API	2208
Java batch persistence configuration . . . . .	2209
Securing the Liberty batch environment . . . . .	2210
Java batch shutdown and recovery . . . . .	2213
Batch REST API . . . . .	2213
Enabling multiple server support by using the Liberty embedded messaging provider . . . . .	2227
Enabling multiple server support by using the WebSphere MQ messaging provider . . . . .	2229
Enabling multiple server partitions support by using the WebSphere MQ messaging provider . . . . .	2233
Enabling multiple server partitions support by using the Liberty embedded messaging provider. . . . .	2239
Enabling batch job events publishing . . . . .	2243
batchManager command-line client utility . . . . .	2246
Configuring the batchManagerZos client utility	2249
Viewing Java batch job logs . . . . .	2252
Liberty: Shared libraries . . . . .	2254
Loose applications . . . . .	2255
Discovering REST API documentation on a Liberty server . . . . .	2260
Subscribe to Liberty REST API updates . . . . .	2263

Subscribing to Liberty REST API updates in a collective . . . . .	2264
REST endpoints for pushing APIs into IBM API Connect . . . . .	2265

## **Chapter 11. Monitoring the Liberty server runtime environment . . . . . 2267**

Liberty:JVM monitoring . . . . .	2267
Liberty:Web application monitoring . . . . .	2268
Liberty:ThreadPool monitoring . . . . .	2269
Liberty:JAX-WS monitoring . . . . .	2270
SIP application monitoring . . . . .	2271
Liberty:Sessions monitoring . . . . .	2286
Liberty:ConnectionPool monitoring. . . . .	2287
Liberty:Multiple components monitoring. . . . .	2288
Liberty:HTTP access logging . . . . .	2289
HTTP access log settings . . . . .	2289
HTTP access log format . . . . .	2289

## **Chapter 12. Tuning Liberty . . . . . 2291**

Tuning Liberty for secure applications. . . . .	2293
Tuning federated LDAP repositories in Liberty	2295

## **Chapter 13. Liberty:Troubleshooting tips . . . . . 2297**

Security bulletins for the Liberty profile . . . . .	2309
Logstash collector . . . . .	2309
Using the Logstash collector . . . . .	2311
Liberty:Logging and Trace. . . . .	2313
Viewing trace and message log files by using developer tools . . . . .	2317
Liberty: Timed operations and JDBC calls . . . . .	2318
Event Logging . . . . .	2319
Slow and hung request detection . . . . .	2321
Liberty:Binary logging . . . . .	2323
BinaryLog command options. . . . .	2327
Configuring binary logging in Liberty. . . . .	2331
Liberty:Runtime environment known issues and restrictions . . . . .	2333
Liberty: Developer Tools known issues and restrictions . . . . .	2342
Liberty:Messages . . . . .	2344
Liberty: Abend reason codes . . . . .	2347
Troubleshooting OSGi applications by using developer tools . . . . .	2348
Troubleshooting Session Initiation Protocol (SIP) on Liberty . . . . .	2349
Troubleshooting the SIP container session repository on Liberty . . . . .	2349
Tracing a Session Initiation Protocol (SIP) container on Liberty. . . . .	2352
Session Initiation Protocol (SIP) binary log and trace extensions on Liberty . . . . .	2353

## **Index . . . . . 2355**



---

## Chapter 1. Liberty overview

Liberty is a highly composable, fast to start, dynamic application server runtime environment.

You can install the server as described in “Installing and uninstalling Liberty using downloaded files and archives” on page 1371.

Because Liberty does not include a Java™ runtime environment (JRE), you must install a compliant Java implementation (JRE or SDK) beforehand. For more information about supported Java environments, and where to get them, see “Minimum supported Java levels” on page 2333.

This server supports two models of application deployment:

- Deploy an application by dropping it into the `dropins` directory.
- Deploy an application by adding it to the server configuration file.

Liberty supports a subset of the following parts of the full WebSphere® Application Server programming model:

- Web applications
- OSGi applications
- **8.5.5.0** Enterprise JavaBeans (EJB) applications

Associated services such as transactions and security are available to these application types.

Features are the units of functionality by which you control the pieces of the runtime environment that are loaded into a particular server. For a list of the main Liberty features, see “Liberty features” on page 826.

**8.5.5.0** You can also create your own features, as described in Chapter 7, “Extending Liberty,” on page 1771.

**8.5.5.2** You can work with the runtime environment directly, or use the WebSphere Application Server Developer Tools for Eclipse. Further, you can use Admin Center to administer Liberty servers and applications and other resources from a web browser. See Chapter 6, “Administering Liberty,” on page 1555.

On distributed platforms, Liberty provides both a development and an operational environment. On Mac OS, it provides a development environment.

**z/OS** On z/OS® systems, Liberty provides an operations environment. You can work natively with this environment by using the MVS™ console. For application development, consider using the Eclipse-based developer tools on a separate distributed system, or on Mac OS.

You can organize Liberty servers into collectives to support clustering, administration, and other operations that act on multiple Liberty servers at a time in order to efficiently and accurately deliver application services to your organization. See “Liberty: Collective architecture” on page 1450 for more information.

---

## Liberty: zero-migration architecture

With the Liberty zero-migration architecture, you can move to the latest version of Liberty with minimal impact to your current applications and configurations.

Zero-migration architecture means that you can use existing, unmodified configuration and application files with an updated version of the Liberty runtime environment without unwanted or unexpected change in behavior. With the following two aspects of architecture, you almost never need to make changes:

### Full compatibility between product versions

You can update Liberty without migrating your configuration files.

### Pluggable features

Your existing APIs and behaviors are supported in new product versions, and new APIs and behaviors are added in new features.

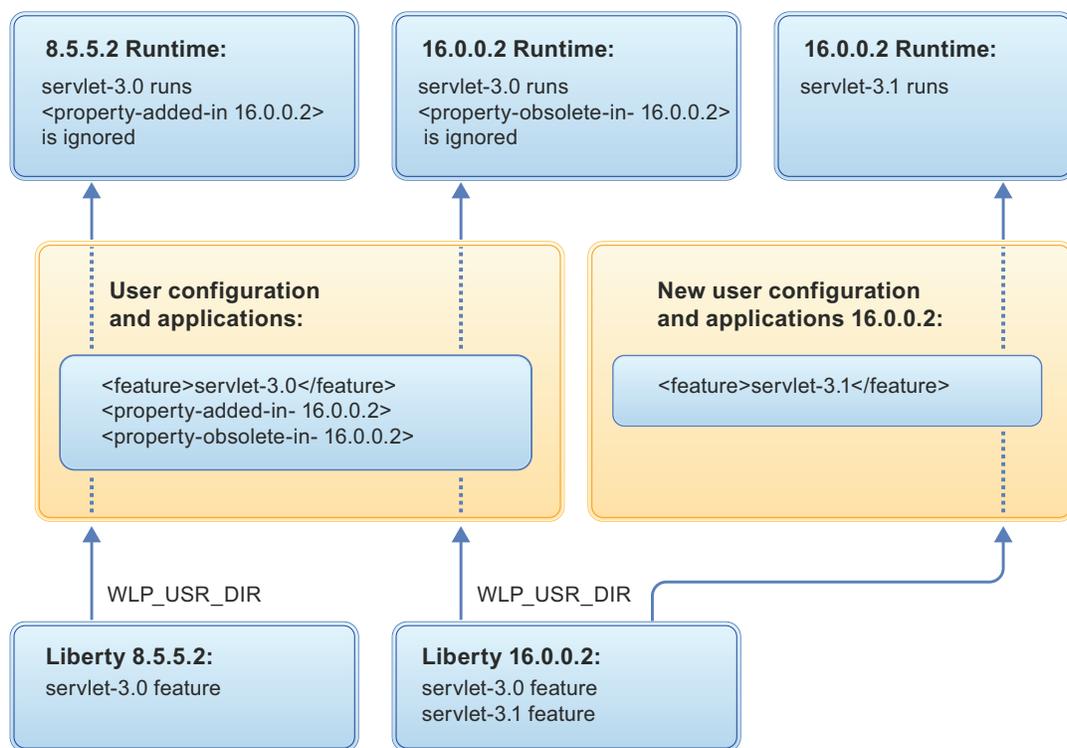
## User configuration files

The Liberty runtime environment never modifies user configuration files, which are fully compatible between versions. You can use a single version of your configuration files across multiple versions. Files that you created for a previous version of Liberty can be used with a later version. Files that you create for later versions can be used with previous versions. As a result, if all configured features are installed, you can use a single set of files across multiple versions without modifications. Any configuration settings that do not apply to a particular version of the Liberty runtime environment are ignored.

## User applications

The Liberty runtime environment uses pluggable features to support multiple versions of an API. For example, both the Servlet 3.0 and 3.1 specifications are supported. Changes in API behavior only happen in new feature versions, so you can choose the appropriate feature version for your application. These versioned features continue to be supported across Liberty updates. If you continue to use the same feature version, you never need to migrate your application.

For example, if your application uses Servlet 3.0, the Liberty server that runs the application must have the `servlet-3.0` feature. You can update Liberty and continue to use the `servlet-3.0` feature indefinitely, regardless of how many other Servlet specification levels are supported. You need to migrate your applications only if you choose to use the `servlet-3.1` feature instead.



If you use third-party APIs, be aware that they can be changed or removed when you update Liberty. Third-party APIs are exposed to applications through Liberty features. Compatibility with an earlier version of these APIs is not controlled by Liberty and is not guaranteed. Some APIs that are available to applications are not provided by Liberty features and do not benefit from this design, so you might need to modify your application code. For example, you might need to update the Java APIs that are provided by the underlying Java SDK. Occasionally, you might need to update the version of the Java SDK. Rather than manually gathering information and migrating your applications, scan your applications for any required changes by using the Migration Toolkit for Application Binaries and the WebSphere Application Server Migration Toolkit. To download the toolkit and get more information, see the *Migration on WASdev*.

## Using new features

If you want to use a new feature, consider the following questions:

### How does a new feature affect existing applications?

A new version of a feature that you are already using might impact your existing applications. For example, if you currently use Servlet 3.0 and you want to use Servlet 3.1, your existing servlet applications might need to be changed to work correctly with Servlet 3.1. Modify your application to work with the new feature version or keep your applications in a server that is configured with the original feature version, such as Servlet 3.0, and create a server configuration with the new version for new applications.

### Is the new feature compatible with existing features?

The product supports mixing some features across different versions of Java EE, but it is simpler to stay within one version of the Java EE specification, if possible. Some features interact closely with other features when they are both configured into the same server, and are sensitive to their versions. For example, many of the Java EE features are closely associated with the features for Contexts and Dependency Injection (CDI) and only work with a specific version of that feature. If you add a feature into your configuration, you might need to change the versions of other features that you are already using. For more information, see *Supported Java EE 6 and 7 feature combinations*.

## Does the new feature require other configuration changes

Some features require specific versions of prerequisite software, most commonly the Java SDK. Java EE 7 features, for example, require Java version 7 as a minimum. Therefore, adding a Java EE 7 feature to your server configuration might require you to move up to Java SDK 7 or later.

## Exceptions to zero-migration

In some rare instances, the zero-migration concept is not followed. In the following scenarios, you might need to modify your application or configuration:

### Security fixes

If a security-related fix is required, but cannot be done safely while preserving existing behavior, then you might need to modify your application or configuration.

### Third-party API requirements

The product does not control APIs from the third-party class loader configuration. As a result, updates to third-party components have no guarantee of compatibility with an earlier version.

### Removal of support

Liberty continues support for parts of the product that affect user data, but it is occasionally necessary to withdraw a feature or supported software product. Usually, users receive removal notifications at least two years in advance. However, notifications are not as practical when other software suppliers remove support for their product earlier than Liberty does. Be aware of the third-party products that you are using with your Liberty installation and of their lifecycle dates. For information about items that are eligible for future removal, see *Removal notices*.

### Undocumented configuration properties

The Liberty code base is common with the WebSphere Application Server full profile code base. Therefore, some configuration properties in the Liberty code base might not be documented, but when specified might affect the behavior of Liberty. As these configuration properties do not apply to Liberty, they are not supported for Liberty. They were not tested for Liberty and might not work reliably in Liberty now or in the future. As these properties are not documented as a product external, they can be removed at any time.

---

## Java EE 7 in Liberty

8.5.5.6

Liberty now supports the full Java Platform, Enterprise Edition (Java EE) 7. Before Version 8.5.5.6, Liberty only supported the Java EE 6 Web Profile. But, now Liberty supports the Java EE 7 full platform. This is a significant improvement and better aligns with the Java EE 6 full platform support available in WebSphere Application Server traditional.

 **Watch:** The Java EE 7 in Liberty video shows what specifications are in Java EE 7 and briefly describes how to enable your Liberty server for Java EE 7 features. [Transcript]

### Benefits of Java EE 7

- Easier delivery of HTML5 dynamic scalable applications for desktops, tablets, and smartphones through Java EE 7 Web Profile

Java EE 6 introduced Web Profile to assist developers of dynamic web applications, providing technologies such as Enterprise JavaBeans (EJB) Lite, Java Persistence API (JPA), and Java Transaction API (JTA).

Java EE 7 Web Profile adds support for HTML5. Two new technologies, WebSocket and JSON, speed up data exchanges and simplify data parsing for portable applications. Updates to existing technologies, JAX-RS 2.0, Java Server Faces (JSF) 2.2, and Servlet 3.1 enhance your ability to develop dynamic HTML5 applications. For example, JAX-RS 2.0 provides asynchronous response processing through scalable, high performance RESTful Services.

- Increased developer productivity  
A simplified application architecture reduces the amount of boilerplate code needed for business logic, such as in JMS 2.0 and the JAX-RS 2.0 client API. A more robust POJO development model enables broader use of annotations, such as in JAX-RS 2.0 Interceptors and Filters and in CDI. Bean Validation 1.1 offers method-level validation.
- Improved support for enterprise demands  
Java EE continues to support enterprise demands with Java EE Connector Architecture (JCA), Java Transaction API (JTA), and Java Message Service (JMS). Java EE 7 introduces the ability to write batch applications in Java that use a standard API and are portable across multiple runtimes. Batch Applications enables better use of computing resources by shifting processing times to when resources are typically idle. Concurrency Utilities enables developers to write scalable applications that integrate with the Java EE runtime in a secure, reliable manner.
- Deprecation of older technologies  
Older technologies are optional: Application Deployment (JSR-88); JAXR, for interfacing with UDDI registries (JSR-93); JAX-RPC, for XML-based RPC (JSR-101); and EJB 2.x Container Managed Persistence, which Java Persistence API (JSR-338) replaces.

## Java EE 7 full platform and Web Profile

The Java EE 7 specification defines the full platform Enterprise Edition. The Web Profile is a properly defined subset of the full platform.

### Web Profile

The Web Profile defines a reasonably complete stack that targets "modern" web applications. This stack is a subset of the full platform standard APIs, capable of addressing the needs of most web applications.

### Full platform

The full platform defines the full complement of the Java EE programming model. Besides the Web Profile features, the full platform has specifications for advanced business capabilities that an enterprise needs, such as for connectivity, security, enterprise beans, messaging, and application clients.

You need to consider these definitions when you install Liberty and its available features. Installation options provide the Liberty runtime (kernel) as well as features that support the full platform or Web Profile. You can choose to install the Liberty kernel with just the Web Profile features or install individual Java EE features to your existing Liberty kernel installation.

You also need to consider the definitions when you deploy applications to a Liberty server. For example, if your Liberty installation supports Web Profile features but your application needs a server that supports enterprise connectivity APIs, you must add full platform features to your Liberty installation or deploy the application to a Liberty installation that has full platform features.

To quickly add support for Java EE to your Liberty server, use either the `webProfile-7.0` or `javaee-7.0` convenience features in the feature manager of your server configuration; for example:

```
<featureManager>
  <feature>javaee-7.0</feature>
</featureManager>
```

A third convenience feature, `javaeeClient-7.0`, is also available to quickly configure an application client component:

```
<featureManager>
  <feature>javaeeClient-7.0</feature>
</featureManager>
```

## Installing a Liberty kernel with Java EE 7 features

The quickest way to install a Liberty runtime with Java EE 7 features is to download a compressed (ZIP) file from the WASdev community download page and extract it into an empty directory. See “Installing Liberty by extracting a ZIP archive file” on page 1381.

You also can install a Liberty runtime with Java EE 7 features by using a developer tool such as WebSphere Application Server Developer Tools for Eclipse. See “Installing Liberty Repository assets” on page 1391.

You can add Java EE 7 features to an existing installation by running the **featureManager** or **installUtility** command. See “Installing Liberty Repository assets” on page 1391.

If you used Installation Manager to install a version of Liberty older than 8.5.5.6, you can use Installation Manager to apply interim fixes that upgrade the installation to Liberty 8.5.5.6 and then install Java EE 7 features. See “Installing and uninstalling Liberty using Installation Manager” on page 1164 and “Installing assets using Installation Manager” on page 1411.

## Resources to help you get started using Java EE 7 technologies

- WASdev website
  - Product and Java EE feature downloads, blogs, videos, samples, articles, and a Q & A forum, dW Answers.
- Architecture topics on Java EE 7
  - “Java EE 7 programming model support” on page 9
  - “Supported Java EE 6 and 7 feature combinations” on page 16
  - “Java EE 7 behavior changes” on page 17
- “Liberty features” on page 826
- “Preparing and running an application client” on page 1445
- “Multimedia” on page 1046
- Java EE 7 specifications
- Java EE 7 samples

---

## Liberty:Architecture

Liberty is a highly composable and dynamic runtime environment. OSGi services are used to manage component lifecycles, and the injection of dependencies and configuration. The server process comprises a single JVM, the Liberty kernel, and any number of optional features. The feature code and most of the kernel code runs as OSGi bundles within an OSGi framework. Features provide the programming models and services that are required by applications.

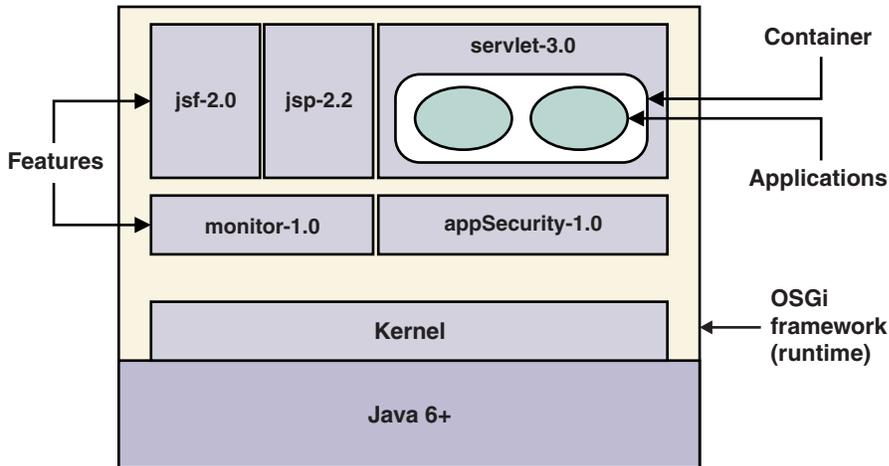


Figure 1. Liberty architecture

The kernel launcher bootstraps the system and starts the OSGi framework. The configuration is parsed, and then the configured features are loaded by the feature manager. The kernel extensively uses OSGi services to provide a highly dynamic runtime environment. The OSGi Configuration Admin service manages system configuration, and an OSGi Declarative Services component manages the lifecycle of system services. The file monitor service detects application and configuration file changes, and the logging service writes messages and debug information to the local file system.

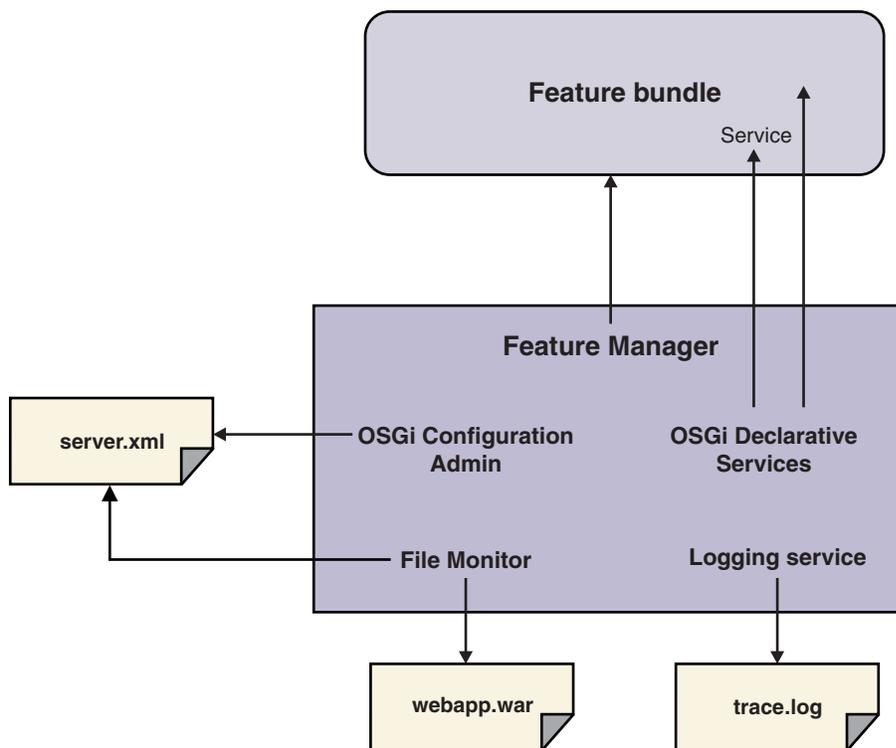


Figure 2. Liberty kernel

Features are specified in the system configuration files that are the `server.xml` file and any other included files. The server configuration files populate the OSGi Configuration Admin service, which injects the feature configuration into the feature manager service. The feature manager maps each feature name to a

list of bundles that provide the feature. The bundles are installed into the OSGi framework and started. The feature manager responds to configuration changes by dynamically adding and removing features while the server is running.

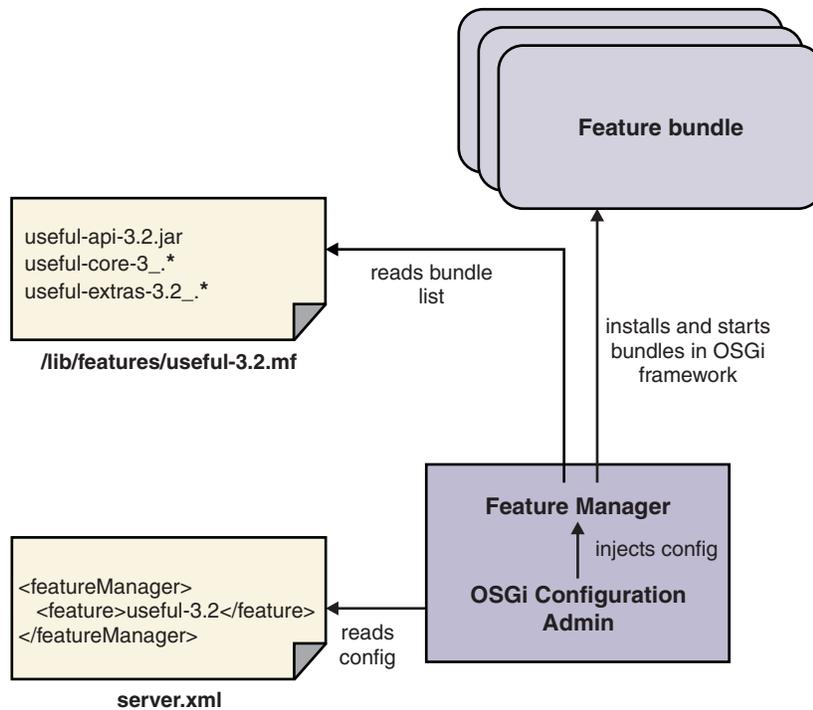


Figure 3. Feature management

Runtime services provide configuration default settings so that the configuration you need to specify is kept to a minimum. You specify the features you need, along with any additions or overrides to the system default settings, in a `server.xml` file. You might choose to structure your configuration into a number of separate files that are linked to the parent `server.xml` file by using an “include” syntax. At server startup, or when the user configuration files are changed, the kernel configuration management parses your configuration and applies it over the system default settings. The set of configuration properties that belongs to each service is injected into the service each time the configuration is updated.

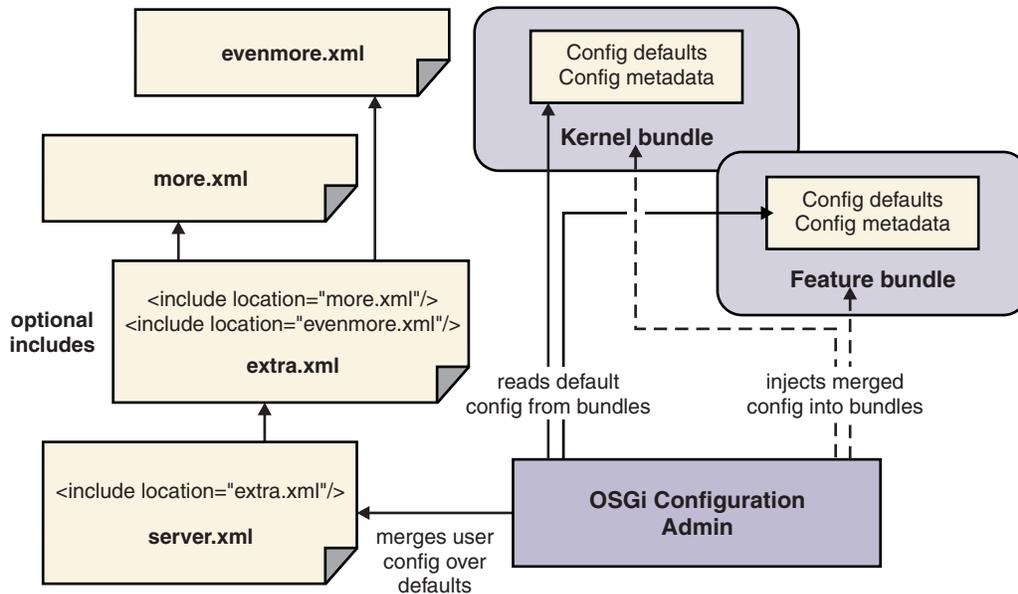


Figure 4. Configuration management

The OSGi Declarative Services component is used so that function can be decomposed into discrete services, which are activated only when needed. This behavior helps the runtime environment to be “late and lazy”, keeping the footprint small and the startup fast. Declared services are added to the OSGi service registry, and dependencies between services can be resolved without loading implementation classes. Service activation can be delayed until a service is used: when the service reference is resolved. Configuration for each service is injected as the service is activated, and is reinjected if the configuration is later modified.

## Java EE 7 programming model support

Liberty complies with Java Platform, Enterprise Edition (Java EE) 7. The Java EE 7 table and links show the extent to which each of the major server profiles supports the full WebSphere Application Server programming model.

### Java EE 7 technologies

Table 1. Java EE 7 support by profile.

A list of Java EE technologies, subdivided into sections for web services, web applications, enterprise applications, management and security, and Java EE-related specifications in Java SE. For each technology there is a specification reference, any related Liberty feature, and an indication of whether the technology is supported by the full profile, the Liberty profile, and Liberty Core.

Technology	Specification reference	Liberty feature	Full profile	Liberty profile	Liberty Core
Java Platform, Enterprise Edition 7 (Java EE 7)	JSR 342	javaee-7.0 javaeeClient-7.0		8.5.5.6	
Java Platform, Enterprise Edition 7 Web Profile	JSR 342	webProfile-7.0		8.5.5.6	8.5.5.6
Web services technologies					

Table 1. Java EE 7 support by profile (continued).

A list of Java EE technologies, subdivided into sections for web services, web applications, enterprise applications, management and security, and Java EE-related specifications in Java SE. For each technology there is a specification reference, any related Liberty feature, and an indication of whether the technology is supported by the full profile, the Liberty profile, and Liberty Core.

Technology	Specification reference	Liberty feature	Full profile	Liberty profile	Liberty Core
Java API for RESTful Web Services (JAX-RS) 2.0	JSR 339	jaxrs-2.0		8.5.5.6	8.5.5.6
Implementing Enterprise Web Services 1.4	JSR 109			8.5.5.4	
Java API for XML-Based Web Services (JAX-WS) 2.2	JSR 224	jaxws-2.2		8.5.5.0	
Web Services Interoperability Organization (WS-I) Basic Profile	WS-I Basic Profile 1.2 WS-I Basic Profile 2.0	jaxws-2.2		8.5.5.0	
Java Architecture for XML Binding (JAXB) 2.2	JSR 222	jaxb-2.2		8.5.5.0	
Web Services Metadata for the Java Platform	JSR 181			8.5.5.0	
Java API for XML-based RPC (JAX-RPC) 1.1 (Optional)	JSR 101				
Java API for WSDL (JWSDL)	JSR 110			8.5.5.0	
SOAP with Attachments API for Java (SAAJ) 1.3(SOAP with Attachments API for Java (SAAJ) is also referred to as <i>Java APIs for XML Messaging</i> .)	JSR 67			8.5.5.0	8.5.5.0
Java API for XML Registries (JAXR) 1.0 (Optional)	JSR 93				
<b>Web application technologies</b>					
Java API for JSON Processing (JSON-P) 1.0	JSR 353	jsonp-1.0		8.5.5.4	8.5.5.4
Java Servlet 3.1	JSR 340	servlet-3.1		8.5.5.4	8.5.5.4
JavaServer Faces (JSF) 2.2	JSR 344	jsf-2.2		8.5.5.6	8.5.5.6
JavaServer Pages 2.3	JSR 245	jsp-2.3		8.5.5.5	8.5.5.5

Table 1. Java EE 7 support by profile (continued).

A list of Java EE technologies, subdivided into sections for web services, web applications, enterprise applications, management and security, and Java EE-related specifications in Java SE. For each technology there is a specification reference, any related Liberty feature, and an indication of whether the technology is supported by the full profile, the Liberty profile, and Liberty Core.

Technology	Specification reference	Liberty feature	Full profile	Liberty profile	Liberty Core
Expression Language (JSP/EL) 3.0	JSR 341	el-3.0		8.5.5.5	8.5.5.5
Standard Tag Library for JavaServer Pages (JSTL) 1.2	JSR 52				
Debugging Support for Other Languages 1.0	JSR 45				
WebSocket 1.1	JSR 356	websocket-1.1		8.5.5.5	8.5.5.5
WebSocket 1.0	JSR 356	websocket-1.0		8.5.5.4	8.5.5.4
<b>Enterprise application technologies</b>					
EE Concurrency Utilities 1.0	JSR 236	concurrent-1.0		8.5.5.4	8.5.5.4
Contexts and Dependency Injection for Java (Web Beans) 1.2	JSR 346	cdi-1.2		8.5.5.6	8.5.5.6
Contexts and Dependency Injection for Java (Web Beans) 1.1	JSR 346	cdi-1.2(Java EE 7 defines CDI 1.1. The CDI maintenance release CDI 1.2. The cdi-1.2 feature supports both CDI 1.1 and CDI 1.2.)		8.5.5.6	8.5.5.6
Dependency Injection for Java 1.0	JSR 330			8.5.5.0	8.5.5.0
Bean Validation 1.1	JSR 349	beanValidation-1.1		8.5.5.6	8.5.5.6
Enterprise JavaBeans (EJB) 3.2 full	JSR 345	ejb-3.2(The ejb-3.2 feature includes the following EJB sub-features: ejbLite-3.2, ejbHome-3.2, ejbPersistentTimer-3.2, ejbRemote-3.2, and mdb-3.2.)		8.5.5.6	
Enterprise JavaBeans (EJB) 3.2 Lite	JSR 345	ejbLite-3.2		8.5.5.6	8.5.5.6
Interceptors 1.2	JSR 318			8.5.5.6	8.5.5.6
Java EE Connector Architecture (JCA) 1.7	JSR 322	jca-1.7		8.5.5.6	

Table 1. Java EE 7 support by profile (continued).

A list of Java EE technologies, subdivided into sections for web services, web applications, enterprise applications, management and security, and Java EE-related specifications in Java SE. For each technology there is a specification reference, any related Liberty feature, and an indication of whether the technology is supported by the full profile, the Liberty profile, and Liberty Core.

Technology	Specification reference	Liberty feature	Full profile	Liberty profile	Liberty Core
Java Persistence 2.1	JSR 338	jpa-2.1		8.5.5.6 	8.5.5.6 
Common Annotations for the Java Platform 1.2 (Common Annotations 1.2 added the javax.annotation.Priority single annotation type, which Contexts and Dependency Injection 1.2 uses. For information about CDI 1.2, see "Contexts and Dependency Injection 1.2" on page 868.)	JSR 250			8.5.5.6 	8.5.5.6 
Java Message Service (JMS) API 2.0	JSR 343	jms-2.0		8.5.5.6 	
Java Transaction API (JTA) 1.2	JSR 907			8.5.5.6 	8.5.5.6 
JavaMail 1.5	JSR 919	javaMail-1.5		8.5.5.6 	8.5.5.6 
Batch Applications for Java Platform 1.0	JSR 352	batch-1.0		8.5.5.6 	
<b>Management and security technologies</b>					
Java Authentication Service Provider Interface for Containers (JASPIC) 1.1	JSR 196	jspic-1.1		8.5.5.6 	8.5.5.9 
Java Authorization Contract for Containers (JACC) 1.5	JSR 115	jacc-1.5		8.5.5.6 	8.5.5.9 
Java EE Application Deployment 1.2 (Optional)	JSR 88				

Table 1. Java EE 7 support by profile (continued).

A list of Java EE technologies, subdivided into sections for web services, web applications, enterprise applications, management and security, and Java EE-related specifications in Java SE. For each technology there is a specification reference, any related Liberty feature, and an indication of whether the technology is supported by the full profile, the Liberty profile, and Liberty Core.

Technology	Specification reference	Liberty feature	Full profile	Liberty profile	Liberty Core
J2EE Management 1.1 (To invoke Management EJB APIs, the server configuration must have both the j2eeManagement-1.1 and ejbRemote-3.2 features in a feature manager. After both features are in the server configuration, you can invoke Management EJB API through JNDI name lookup. The Management EJB binding name (JNDI lookup name) is ejb/mejb/MEJB.)	JSR 77	j2eeManagement-1.1	△	8.5.5.6 △	
<b>Java EE-related specifications in Java SE</b>					
Java API for XML Processing (JAXP) 1.4	JSR 206		△	△	△
Java Database Connectivity (JDBC) 4.1	JSR 221	jdbc-4.1		8.5.5.5 △	8.5.5.5 △
Java Management Extensions (JMX) 2.0	JSR 255		△	△	△
JavaBeans Activation Framework (JAF) 1.1	JSR 925		△	△	△
Streaming API for XML (StAX) 1.0	JSR 173		△	△	△

## Programming model extensions

For a list of WebSphere programming model extensions, see "WebSphere extensions" in the WebSphere Application Server: Overview and quick start topic.

## Java EE 6 programming model support

The Java EE 6 table and links show the extent to which each of the major server profiles supports the full WebSphere Application Server programming model.

## Java EE 6 technologies

Table 2. Java EE 6 support by profile.

A list of Java EE technologies, subdivided into sections for web services, web applications, enterprise applications, management and security, and Java EE-related specifications in Java SE. For each technology there is a specification reference, any related Liberty feature, and an indication of whether the technology is supported by the full profile, by the Liberty profile, and by Liberty Core. The Liberty Core edition contains a subset of the Liberty features that are available in the other product editions.

Technology	Specification reference	Liberty feature	Full profile	Liberty profile	Liberty Core
Java Platform, Enterprise Edition 6 (Java EE 6)	JSR 316		△		
Java Platform, Enterprise Edition 6 Web Profile	JSR 316	webProfile-6.0	△	△	△
<b>Web services technologies</b>					
Java API for RESTful Web Services (JAX-RS) 1.1	JSR 311	jaxrs-1.1	△	△	△
Implementing Enterprise Web Services 1.4	JSR 109		△	<b>8.5.5.0</b> △	
Java API for XML-Based Web Services (JAX-WS) 2.2	JSR 224	jaxws-2.2	△	<b>8.5.5.0</b> △	
Web Services Interoperability Organization (WS-I) Basic Profile	WS-I Basic Profile 1.2 WS-I Basic Profile 2.0	jaxws-2.2	△	<b>8.5.5.0</b> △	
Java Architecture for XML Binding (JAXB) 2.2	JSR 222	jaxb-2.2	△	<b>8.5.5.0</b> △	
Web Services Metadata for the Java Platform	JSR 181		△	<b>8.5.5.0</b> △	
Java API for XML-based RPC (JAX-RPC) 1.1	JSR 101		△		
Java API for WSDL (JWSDL)	JSR 110		△	<b>8.5.5.0</b> △	
SOAP with Attachments API for Java (SAAJ) 1.3(SOAP with Attachments API for Java (SAAJ) is also referred to as <i>Java APIs for XML Messaging</i> .)	JSR 67		△	<b>8.5.5.0</b> △	
Java API for XML Registries (JAXR) 1.0	JSR 93		△		

Table 2. Java EE 6 support by profile (continued).

A list of Java EE technologies, subdivided into sections for web services, web applications, enterprise applications, management and security, and Java EE-related specifications in Java SE. For each technology there is a specification reference, any related Liberty feature, and an indication of whether the technology is supported by the full profile, by the Liberty profile, and by Liberty Core. The Liberty Core edition contains a subset of the Liberty features that are available in the other product editions.

Technology	Specification reference	Liberty feature	Full profile	Liberty profile	Liberty Core
<b>Web application technologies</b>					
Java Servlet 3.0	JSR 315	servlet-3.0	△	△	△
JavaServer Faces (JSF) 2.0	JSR 314	jsf-2.0	△	△	△
JavaServer Pages 2.2/Expression Language (JSP/EL) 2.2	JSR 245	jsp-2.2	△	△	△
Standard Tag Library for JavaServer Pages (JSTL) 1.2	JSR 52		△	△	△
Debugging Support for Other Languages 1.0	JSR 45		△	△	△
<b>Enterprise application technologies</b>					
Contexts and Dependency Injection for Java (Web Beans 1.0)	JSR 299	cdi-1.0	△	△	△
Dependency Injection for Java 1.0	JSR 330		△	<b>8.5.5.0</b> △	△
Bean Validation 1.0	JSR 303	beanValidation-1.0	△	△	△
Enterprise JavaBeans (EJB) 3.1 (includes Interceptors 1.1)	JSR 318	ejbLite-3.1	△	<b>8.5.5.0</b> △(The Liberty supports only the EJB Lite subset and Message Driven Beans. See the “Enterprise JavaBeans (EJB) Lite subset” section of “Liberty features” on page 826.)	<b>8.5.5.0</b> △(Liberty supports only the EJB Lite subset and Message Driven Beans. See the “Enterprise JavaBeans (EJB) Lite subset” section of “Liberty features” on page 826.)
Java EE Connector Architecture 1.6	JSR 322	jca-1.6	△	<b>8.5.5.2</b> △	
Java Persistence 2.0	JSR 317		△	△	△
Common Annotations for the Java Platform 1.1	JSR 250		△	△	△
Java Message Service (JMS) API 1.1	JSR 914	jms-1.1	△	<b>8.5.5.0</b> △	

Table 2. Java EE 6 support by profile (continued).

A list of Java EE technologies, subdivided into sections for web services, web applications, enterprise applications, management and security, and Java EE-related specifications in Java SE. For each technology there is a specification reference, any related Liberty feature, and an indication of whether the technology is supported by the full profile, by the Liberty profile, and by Liberty Core. The Liberty Core edition contains a subset of the Liberty features that are available in the other product editions.

Technology	Specification reference	Liberty feature	Full profile	Liberty profile	Liberty Core
Java Transaction API (JTA) 1.1	JSR 907		△	△	△
JavaMail 1.4	JSR 919		△		
<b>Management and security technologies</b>					
Java Authentication Service Provider Interface for Containers (JASPIC)	JSR 196		△		
Java Authorization Contract for Containers (JACC) 1.3	JSR 115		△		
Java EE Application Deployment 1.2	JSR 88		△		
J2EE Management 1.1	JSR 77		△		
<b>Java EE-related specifications in Java SE</b>					
Java API for XML Processing (JAXP) 1.4	JSR 206		△	△	△
Java Database Connectivity (JDBC) 4.0	JSR 221	jdbc-4.0	△	△	△
Java Management Extensions (JMX) 2.0	JSR 255		△	△	△
JavaBeans Activation Framework (JAF) 1.1	JSR 925		△	△	△
Streaming API for XML (StAX) 1.0	JSR 173		△	△	△

## Programming model extensions

For a list of WebSphere programming model extensions, see "WebSphere extensions" in the WebSphere Application Server: Overview and quick start topic.

## Supported Java EE 6 and 7 feature combinations

8.5.5.6

Some combinations of Java EE 7 and Java EE 6 Liberty features in a server configuration are compatible. However, many combinations are not compatible and cause an error when the server starts.

The error message resembles:

CWWKF0033E: The singleton features com.ibm.websphere.appserver.javaeeCompatible-6.0 and com.ibm.websphere.appserver.javaeeCompat

The following table marks compatible feature combinations with a checkmark (△). Ensure that your server configuration does not contain incompatible features.

*Table 3. Supported combinations of Java EE 7 and Java EE 6 Liberty features.* Java EE 7 features are listed vertically. Java EE 6 features are listed horizontally. A checkmark (△) indicates that the combination of Java EE 7 and 6 features is supported and a server configuration can contain both features. An empty cell (no △) indicates that the combination of Java EE 7 and 6 features is not supported.

Java EE 7 features	Java EE 6 features														
	beanValidation-1.0	cdi-1.0	ejbLite-3.1	jaxb-2.2	jaxrs-1.1	jaxws-2.2	jca-1.6	jdbc-4.0	jms-1.1	jpa-2.0	jsf-2.0	jsp-2.2	managed-Beans-1.0	mdb-3.1	servlet-3.0
batch-1.0				△		△		△		△			△		
beanValidation-1.1				△		△		△		△			△		
cdi-1.2				△		△		△		△			△		
concurrent-1.0	△	△	△	△	△	△	△	△	△	△	△	△	△	△	△
el-3.0	△	△	△	△	△	△	△	△	△	△	△	△	△	△	△
ejb-3.2				△		△				△			△		
ejbLite-3.2				△		△		△		△			△		
javaMail-1.5	△	△	△	△	△	△	△	△	△	△	△	△	△	△	△
jacc-1.5	△	△	△	△	△	△	△	△	△	△	△	△	△	△	△
jaspic1.1	△	△	△	△	△	△	△	△	△	△	△	△	△	△	△
jaxrs-2.0				△		△		△		△			△		
jca-1.7				△		△		△		△			△		
jdbc-4.1	△	△	△	△	△	△	△	△	△	△	△	△	△	△	△
jms-2.0				△		△		△		△			△		
jpa-2.1				△		△				△			△		
jsf-2.2				△				△		△			△		
jsonp-1.0	△	△	△	△	△	△	△	△	△	△	△	△	△	△	△
jsp-2.3	△	△	△	△	△	△	△	△	△	△	△	△	△	△	△
mdb-3.2				△		△		△		△			△		
servlet-3.1	△	△	△	△	△	△	△	△	△	△	△	△	△	△	△
websocket-1.0	△	△	△	△	△	△	△	△	△	△	△	△	△	△	△
websocket-1.1	△	△	△	△	△	△	△	△	△	△	△	△	△	△	△

The table shows that the `servlet-3.0` feature of Java EE 6 is incompatible with the `websocket-1.1` feature of Java EE 7. Thus, a server configuration with the following features causes an error:

```
<featureManager>
  <feature>servlet-3.0</feature>
  <feature>websocket-1.1</feature>
</featureManager>
```

To resolve the error, use `servlet-3.1` instead of `servlet-3.0` in the server configuration. The `servlet-3.1` feature is compatible with the `websocket-1.1` feature.

For more information on compatibility, or toleration, of features, see [Tolerating features](#).

## Java EE 7 behavior changes

If you previously incorporated Java Platform, Enterprise Edition (Java EE) 6 features in your Liberty environment, you might encounter behavior changes when you move to a Java EE 7 feature.

You can choose between the Java EE 6 and Java EE 7 feature implementations for each server instance, with consideration for behavior changes. If the required behavior is contained in the Java EE 7 feature only, you must use the Java EE 7 feature. If an existing application would be adversely impacted by behavior changes in the Java EE 7 feature, using the Java EE 6 feature preserves the existing behavior for

that application. You must ensure that the Java EE implementation that you choose is compatible with other Java EE features in your server; for more information, see “Supported Java EE 6 and 7 feature combinations” on page 16.

*Table 4. Features that have Java EE 6 and 7 implementations*

Technology	Java EE 6 feature	Java EE 7 feature	Behavior changes
Bean Validation	beanValidation-1.0	beanValidation-1.1	No behavior changes.
Contexts and Dependency Injection for Java (CDI)	cdi-1.0	cdi-1.2	See “Contexts and Dependency Injection 1.2 behavior changes” on page 1726.
Enterprise JavaBeans (EJB)	ejbLite-3.1	ejbLite-3.2	No behavior changes.
Expression Language (EL)	Included as part of jsp-2.2	el-3.0	See “Expression Language 3.0 feature functions” on page 1722.
Java API for RESTful Web Services (JAX-RS)	jaxrs-1.1	jaxrs-2.0	See “JAX-RS 2.0 behavior changes” on page 2167.
Java EE Connector Architecture (JCA)	jca-1.6	jca-1.7	No behavior changes.
Java Database Connectivity (JDBC)	jdbc-4.0	jdbc-4.1	No behavior changes.
Java Message Service (JMS)	jms-1.1	jms-2.0	No behavior changes.
	wasJmsClient-1.1	wasJmsClient-2.0	See “JMS messaging (wasJmsClient-2.0) behavior changes” on page 1014.
	wmqJmsClient-1.1	wmqJmsClient-2.0	See SupportMQExtensions property.
Java Persistence API (JPA)	jpa-2.0	jpa-2.1	See “Java Persistence API 2.1 behavior changes” on page 1017.
Java Servlet	servlet-3.0	servlet-3.1	See “Servlet 3.1 behavior changes” on page 1714.
Java Transaction API (JTA)	transaction-1.1 (protected feature)	transaction-1.2 (protected feature)	No behavior changes.
JavaServer Faces (JSF)	jsf-2.0	jsf-2.2	See “Configuring Liberty for JavaServer Faces 2.2” on page 1722.
JavaServer Pages (JSP)	jsp-2.2	jsp-2.3	No behavior changes.
Message Driven Beans (MDB)	mdb-3.1	mdb-3.2	No behavior changes.

## Enterprise OSGi programming model support

The Enterprise OSGi table and links show the extent to which each of the major server profiles supports the full WebSphere Application Server programming model.

## Enterprise OSGi technologies

Table 5. Enterprise OSGi support by profile.

A list of enterprise OSGi technologies, subdivided into sections for blueprint, web, and other enterprise technologies. For each technology there is a specification reference, and an indication of whether the technology is supported by the full profile, by the Liberty profile, and by Liberty Core.

Technology	Specification reference	Full profile	Liberty profile	Liberty Core
<b>Blueprint-related technologies</b>				
Blueprint Container	R4.2 Enterprise Chapter 121	△	△	△
Blueprint Transactions		△	△	△
Blueprint Managed JPA		△	△	△
Blueprint Security		△		
Blueprint Resource References		△		
Custom Blueprint Namespaces			8.5.5.4 △	8.5.5.4 △
<b>Web-related technologies</b>				
Web Application Bundles	R4.2 Enterprise Chapter 128	△	△	△
8.5.5.7 WebSocket Applications			8.5.5.7 △	
JNDI	R4.2 Enterprise Chapter 126	△	△	△
JSP		△	△	△
JSTL		△	△	△
JSF		△	△	△
JAX-RS		△	△	△
<b>Other enterprise technologies</b>				
EJB Bundles		△(EJB levels earlier than 3.0 are not supported.)		
Remote Services	R4.2 Compendium Chapter 13	△		
SCA Configuration Type Specification	R4.2 Enterprise Chapter 129	△		
Remote Bundle Repositories		△	△	△
SIP		△(SIP annotations are not supported.)		
Local OSGi application integration			8.5.5.5 △	8.5.5.5 △

**Note:** 8.5.5.7 WebSockets is currently only supported on Liberty.

## Liberty externals support

External functions and resources of Liberty can be used directly, and can be relied on to be in the next release. Internal or incidental aspects of Liberty might change when you apply service, or upgrade to a future release.

### What can I use directly in Liberty and rely on being in the next release?

The following resources can be used directly and will continue to be available in the next release:

- The application programming interfaces (APIs) and system programming interfaces (SPIs) defined by the content of the JAR files in the `${wlp.install.dir}/dev` directories.
  - The application class loader has visibility to the API that is provided by the features in your server configuration. Product extension features have visibility to all API and SPI that is provided by the features in your server configuration.
  - Compile your code against the JAR files in the `${wlp.install.dir}/dev` directories. The JAR files in the `${wlp.install.dir}/dev` directories are provided only for compilation of applications and features, they are not supported for runtime use. Do not use these JAR files in applications, libraries, or tests.
- The server configuration, including features with *public* or *protected* visibility. Public features and configuration elements can be specified in the `server.xml` file and included files; protected features can be included in your own features.
- Commands, scripts and archives in the `${wlp.install.dir}/bin` directory and subdirectories.
- Client utilities in the `${wlp.install.dir}/clients` directory and subdirectories.

## What should I avoid dependencies on?

Do not build dependencies on incidental aspects of the product, or you might be impacted when you apply service or upgrade to future releases. Examples of product internals that you should avoid relying on include, but are not restricted to, the following scenarios:

- The names of product binary jars, for example those in the `${wlp.install.dir}/dev` directory. Compile your code against these JAR files by using the tools or the `javac -extdirs` option.

8.5.5.4

If you are using Apache Ant to compile your code, use wildcards to avoid dependencies on the specific JAR version; for example:

```
<fileset dir="${wlp.install.dir}/dev/api/spec" includes="com.ibm.ws.javaee.servlet.3.0_*.jar"/>
```

Alternatively, you can use the `featureManager classpath` command to generate a classpath for a specific set of features. See “Overriding classes from the Java SDK” on page 2334.

- Direct use of the product binaries in the `${wlp.install.dir}/lib` directory. The only JAR files that can be directly invoked are in the `${wlp.install.dir}/bin/tools` directory.
- Messages that are output by the server at run time. The text and inserts of messages are subject to change in service and version upgrades. As far as practically possible, the product will be consistent in the message IDs that are output at particular points of operation, but this cannot be guaranteed because underlying implementations might change.
- The layout of the product installation, other than the `${wlp.install.dir}/bin` and `${wlp.install.dir}/dev` directories.
- Examples and template files in the `${wlp.install.dir}/templates` directory. These files might be modified when you apply services to your installation.
- Private or third party Java packages that are not explicitly exposed as APIs. These are not visible to the application class loader at run time.
- Do not use the `console.log` file for the automated processing of server output. Instead, use the `messages.log` file for accessing and processing the messages, which provides more detailed information, in a format that is easier to process.

## What might be modified by applying service or an upgrade?

The contents of the following directories and their subdirectories might be modified when service or upgrade is applied. Do not make your own modifications to files in these locations, or they might be overwritten by product maintenance or upgrade:

- `${wlp.install.dir}/bin`
- `${wlp.install.dir}/clients`
- `${wlp.install.dir}/dev`

- `${wlp.install.dir}/java`
- `${wlp.install.dir}/lib`
- `${wlp.install.dir}/templates`

No modifications are made to the contents of the following directories. These are your files, and applying service or upgrade will not modify them:

- `${wlp.install.dir}/etc` (where you might have added a `server.env` or `jvm.options` file).
- `${wlp.install.dir}/usr` (the default location for user configuration and applications).
- Any non-default directory that you designate through the `WLP_USER_DIR` environment variable.

**IBM i** There is an exception to the policy that no modifications are made to the contents of `${wlp.install.dir}/etc`. The file `${wlp.install.dir}/etc/default.env` is created when you install Liberty on IBM® iSeries Platforms using the Installation Manager. This file is also created or replaced by the `iAdmin POSTINSTALL` command during archive and Job Manager installations. The `iAdmin` command is in the `${wlp.install.dir}/lib/native/os400/bin` directory. See “Liberty: iAdmin command” on page 1572.

Third-party APIs might change over time without consideration to backward compatibility. These are Java packages that are considered part of the implementation of features developed in open source communities and delivered as part of Liberty. Third-party APIs are not visible to applications by default; Java EE applications with a classloader configuration that explicitly allows third-party access will have visibility to those packages on the application class loader, and OSGi applications must explicitly import the packages. Consider the impact of incompatible changes before deciding to use third-party APIs.

---

## Liberty:Server configuration

Liberty is configured by exception. The runtime environment operates from a set of built-in configuration default settings, and you only need to specify configuration that overrides those default settings. You do this by editing either the `server.xml` file or another XML file that is included in `server.xml` at run time.

The configuration has the following characteristics:

- Described in XML files.
- Human-readable, and editable in a text editor.
- Small, easy to back up, and easy to copy to another system.
- Shareable across an application development team.
- Composable, so that features can easily add their own configuration to the system.
- Extensibly-typed, so you don't have to modify the current configuration to work with later versions of the runtime environment.
- Dynamically responsive to updates.
- Forgiving, so that missing values are assumed and unrecognized properties are ignored.

Features are the units of functionality by which you control the pieces of the runtime environment that are loaded into a particular server. They are the primary mechanism that makes the server composable. The list of features that you specify in the server configuration provides a functional server. See “Liberty features” on page 826.

When you first install and start the server, a feature manager and a default server configuration are available:

- By default, a server contains the `jsp-2.2` feature, to support servlet and JSP applications. You can use the feature manager to add the features that you need.

- Server configuration is by exception. When you specify the features that you need, the default configuration of those features provides a rich environment that is designed to cover most common requirements, therefore you only need to specify changes from the default configuration.

For a full list of the elements that you can configure to complement or modify the configuration provided by Liberty features, see “Liberty features” on page 826.

You can also use a `bootstrap.properties` file to specify properties that are needed before the main configuration is processed, and to define variables that are used in the main configuration.

For a complete list of configuration files, see Directory locations and properties.

## 8.5.5.0

### Service author perspective: Runtime management of configuration

The Liberty configuration service parses the primary `server.xml` file and any files it includes.

#### 8.5.5.5

The Liberty configuration service also parses the configuration files in the `configDropins` directory.

The Liberty configuration service parses the files, merges the contents over the default configuration values provided by the installed bundles, then feeds the resulting property sets into the OSGi Configuration Admin Service (CA). CA injects each set of properties into the service that owns the set, if it is registered with CA.

The ordering of these steps is flexible. Services can register with CA before or after the initial property sets are established. Properties can be updated in CA after the initial injection, at which time the updated properties are injected into the owning service. It is therefore important that the services can receive, and respond appropriately to, updates to their configuration at any time that the service is active. Specifically, if a service delays its activation until its configuration is available, it must still be able to activate.

To enable a service to receive configuration data, there are a number of steps involved. See “Enabling a service to receive configuration data” on page 1796.

#### z/OS

### Encoding on z/OS

The WLP JVMs are configured to run with a default file encoding of ISO8859-1 (ISO Latin-1). The configuration files that are created by Liberty are tagged in the z/OS file system as text files with an ISO8859-1 encoding. If the z/OS UNIX System Services (USS) automatic code page conversion feature is active, you can use standard editors and text utilities to view and manage configuration files.

For the encoding of log files on z/OS(r) systems, see “Liberty:Logging and Trace” on page 2313.

For more information about USS automatic code page conversion, see Statements and parameters for BPXPRMxx.

### Activation Specification (activationSpec)

Defines an activation specification configuration.

- `authData`

Attribute name	Data type	Default value	Description
authDataRef	A reference to top level authData element (string).		Default authentication data for an activation specification.
id	string		A unique configuration ID.
maxEndpoints	int Minimum: 0	500	The maximum number of endpoints to dispatch to.

### authData

Default authentication data for an activation specification.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## Microsoft Active Directory LDAP Filters (activedLdapFilterProperties)

Specifies the list of default Microsoft Active Directory LDAP filters.

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(objectcategory=group))	An LDAP filter clause for searching the user registry for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	memberOf:member	An LDAP filter that identifies user to group memberships.
id	string		A unique configuration ID.
userFilter	string	(&(sAMAccountName=%v)(objectcategory=user))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	user:sAMAccountName	An LDAP filter that maps the name of a user to an LDAP entry.

## Administered Object (adminObject)

Defines an administered object configuration.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
jndiName	string		JNDI name for a resource.

## Administrator Role (administrator-role)

A collection of users and/or groups assigned the server administrator role.

- group
- user

### group

Group assigned a role.

false

string

### user

User assigned a role.

false

string

## API Discovery (apiDiscovery)

Configuration for the API Discovery feature to document your REST APIs.

- webModuleDoc

Attribute name	Data type	Default value	Description
apiName	string		The name of the aggregated API.
id	string		A unique configuration ID.
maxSubscriptions	int Minimum: 0 Maximum: 100	20	Specifies the maximum number of concurrent REST API clients that are listening for updates.

### webModuleDoc

Configuration for each web module that provides API documentation to be exposed.

false

Attribute name	Data type	Default value	Description
contextRoot	string		The context root of the web module for which you are providing documentation.

Attribute name	Data type	Default value	Description
docURL	string		The URL of the documentation of this web module. The URL can be relative to the context root by starting with a forward slash (/) or absolute by starting with http or https.
enabled	boolean	true	A boolean that controls the processing of documentation for this web module.
id	string		A unique configuration ID.

## Application (application)

Defines the properties of an application.

- application-bnd
  - security-role
    - group
    - run-as
    - special-subject
    - user
- classloader
  - commonLibrary
    - file
    - fileset
    - folder
  - privateLibrary
    - file
    - fileset
    - folder
- resourceAdapter
  - contextService
    - baseContext
      - baseContext
      - classloaderContext
      - jeeMetadataContext
      - securityContext
      - syncToOSThreadContext
      - zosWLMContext
    - classloaderContext
    - jeeMetadataContext
    - securityContext
    - syncToOSThreadContext
    - zosWLMContext
  - customize

Attribute name	Data type	Default value	Description
autoStart	boolean	true	Indicates whether or not the server automatically starts the application.
context-root	string		Context root of an application.
id	string		A unique configuration ID.
location	A file, directory or url.		Location of an application expressed as an absolute path or a path relative to the server-level apps directory.
name	string		Name of an application.
suppressUncoveredHttpMethodWarning	boolean	false	Option to suppress uncovered HTTP method warning message during application deployment.
type	string		Type of application archive.

#### **application-bnd**

Binds general deployment information included in the application to specific resources.

false

Attribute name	Data type	Default value	Description
version	string		Version of the application bindings specification.

#### **application-bnd > security-role**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Name of a security role.

#### **application-bnd > security-role > group**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		Group access ID
id	string		A unique configuration ID.
name	string		Name of a group possessing a security role.

#### **application-bnd > security-role > run-as**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
password	Reversably encoded password (string)		Password of a user required to access a bean from another bean. The value can be stored in clear text or encoded form. To encode the password, use the securityUtility tool with the encode option.
userid	string		ID of a user required to access a bean from another bean.

**application-bnd > security-role > special-subject**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
type	<ul style="list-style-type: none"> <li>• EVERYONE</li> <li>• ALL_AUTHENTICATED_USERS</li> </ul>		One of the following special subject types: ALL_AUTHENTICATED_USERS, EVERYONE.  <b>EVERYONE</b> Everyone  <b>ALL_AUTHENTICATED_USERS</b> All authenticated users

**application-bnd > security-role > user**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		A user access ID in the general form user:realmName/userUniqueId. A value will be generated if one is not specified.
id	string		A unique configuration ID.
name	string		Name of a user possessing a security role.

**classloader**

Defines the settings for an application classloader.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
classProviderRef	List of references to top level resourceAdapter elements (comma-separated string).		List of class provider references. When searching for classes or resources, this class loader will delegate to the specified class providers after searching its own class path.
commonLibraryRef	List of references to top level library elements (comma-separated string).		List of library references. Library class instances are shared with other classloaders.
delegation	<ul style="list-style-type: none"> <li>parentFirst</li> <li>parentLast</li> </ul>	parentFirst	<p>Controls whether parent classloader is used before or after this classloader. If parent first is selected then delegate to immediate parent before searching the classpath. If parent last is selected then search the classpath before delegating to the immediate parent.</p> <p><b>parentFirst</b> Parent first</p> <p><b>parentLast</b> Parent last</p>
privateLibraryRef	List of references to top level library elements (comma-separated string).		List of library references. Library class instances are unique to this classloader, independent of class instances from other classloaders.

### **classloader > commonLibrary**

List of library references. Library class instances are shared with other classloaders.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators

Attribute name	Data type	Default value	Description
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
id	string		A unique configuration ID.
name	string		Name of shared library for administrators

**classloader > commonLibrary > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**classloader > commonLibrary > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**classloader > commonLibrary > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**classloader > privateLibrary**

List of library references. Library class instances are unique to this classloader, independent of class instances from other classloaders.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
id	string		A unique configuration ID.
name	string		Name of shared library for administrators

**classloader > privateLibrary > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**classloader > privateLibrary > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**classloader > privateLibrary > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

### resourceAdapter

Specifies configuration for a resource adapter that is embedded in an application.

false

Attribute name	Data type	Default value	Description
alias	string	\${id}	Overrides the default identifier for the resource adapter. The identifier is used in the name of the resource adapter's configuration properties element, which in turn is used in determining the name of configuration properties elements for any resources provided by the resource adapter. The resource adapter's configuration properties element name has the format, <code>properties.&lt;APP_NAME&gt;.&lt;ALIAS&gt;</code> , where <code>&lt;APP_NAME&gt;</code> is the name of the application and <code>&lt;ALIAS&gt;</code> is the configured alias. If unspecified, the alias defaults to the module name of the resource adapter.
autoStart	boolean		Configures whether a resource adapter starts automatically upon deployment of the resource adapter or lazily upon injection or lookup of a resource.
contextServiceRef	A reference to top level contextService element (string).		Configures how context is captured and propagated to threads.
id	string		Identifies the name of the embedded resource adapter module to which this configuration applies.

### resourceAdapter > contextService

Configures how context is captured and propagated to threads.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
jndiName	string		JNDI name
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**resourceAdapter > contextService > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
id	string		A unique configuration ID.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**resourceAdapter > contextService > baseContext > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

com.ibm.ws.context.service-factory

**resourceAdapter > contextService > baseContext > classloaderContext**

Classloader context propagation configuration.

false

**resourceAdapter > contextService > baseContext > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**resourceAdapter > contextService > baseContext > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**resourceAdapter > contextService > baseContext > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**resourceAdapter > contextService > baseContext > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"><li>• Propagate</li><li>• PropagateOrNew</li><li>• New</li></ul>	Propagate	Indicates how the WLM context should be handled for non-Daemon work. <b>Propagate</b> Use the same WLM Context (if one exists). <b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists. <b>New</b> Always create a new WLM context.

**resourceAdapter > contextService > classloaderContext**

Classloader context propagation configuration.

false

**resourceAdapter > contextService > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**resourceAdapter > contextService > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**resourceAdapter > contextService > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**resourceAdapter > contextService > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"> <li>• Propagate</li> <li>• PropagateOrNew</li> <li>• New</li> </ul>	Propagate	<p>Indicates how the WLM context should be handled for non-Daemon work.</p> <p><b>Propagate</b> Use the same WLM Context (if one exists).</p> <p><b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists.</p> <p><b>New</b> Always create a new WLM context.</p>

**resourceAdapter > customize**

Customizes the configuration properties element for the activation specification, administered object, or connection factory with the specified interface and/or implementation class.

false

Attribute name	Data type	Default value	Description
implementation	string		Fully qualified implementation class name for which the configuration properties element should be customized.
interface	string		Fully qualified interface class name for which the configuration properties element should be customized.

Attribute name	Data type	Default value	Description
suffix	string		Overrides the default suffix for the configuration properties element. For example, "CustomConnectionFactory" in properties.rarModule1.CustomConnectionFa The suffix is useful to disambiguate when multiple types of connection factories, administered objects, or endpoint activations are provided by a resource adapter. If a configuration properties element customization omits the suffix or leaves it blank, no suffix is used.

## Application Manager (applicationManager)

Properties that control the behavior of the application manager

Attribute name	Data type	Default value	Description
autoExpand	boolean	false	Enables automatic extraction of WAR files and EAR files
startTimeout	A period of time with second precision	30s	Specifies how long the server waits for an application to start before it considers it slow. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
stopTimeout	A period of time with second precision	30s	Specifies how long the server waits for an application to stop before it considers it slow. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

## Application Monitoring (applicationMonitor)

Defines how the server responds to application additions, updates, and deletions.

Attribute name	Data type	Default value	Description
dropins	Path to a directory	dropins	Location of the application drop-in directory expressed as an absolute path or a path relative to the server directory.
dropinsEnabled	boolean	true	Monitor the drop-in directory for application additions, updates, and deletions.
pollingRate	A period of time with millisecond precision	500ms	Rate at which the server checks for application additions, updates, and deletions. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
updateTrigger	<ul style="list-style-type: none"> <li>• mbean</li> <li>• polled</li> <li>• disabled</li> </ul>	polled	<p>Application update method or trigger.</p> <p><b>mbean</b> Server will only update applications when prompted by an MBean called by an external program such as an integrated development environment or a management application.</p> <p><b>polled</b> Server will scan for application changes at the polling interval and update any applications that have detectable changes.</p> <p><b>disabled</b> Disables all update monitoring. Application changes will not be applied while the server is running.</p>

## z/OS Connect SMF Audit Interceptor (auditInterceptor)

Defines z/OS Connect's audit interceptor to allow request data to be logged using System Management Facility (SMF) 120 subtype 11 records on z/OS.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
sequence	int Minimum: 0 Maximum: 2147483647	0	The sequence in which this interceptor should be processed with respect to other configured interceptors implementing z/OS Connect's com.ibm.wsspi.zos.connect.Interceptor Service Provider Interface (SPI).

## Authentication Cache (authCache)

Controls the operation of the authentication cache.

Attribute name	Data type	Default value	Description
allowBasicAuthLookup	boolean	true	Allow lookup by user ID and hashed password.
initialSize	int Minimum: 1	50	Initial number of entries supported by the authentication cache.
maxSize	int Minimum: 1	25000	Maximum number of entries supported by the authentication cache.
timeout	A period of time with millisecond precision	600s	Amount of time after which an entry in the cache will be removed. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

## Authentication Data (authData)

Authentication alias for a connection to an Enterprise Information System (EIS) or database.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## Authentication Filter (authFilter)

Specifies a selection rule that represents conditions that are matched against the HTTP request headers to determine whether or not the HTTP request is selected for the authentication.

- host
- remoteAddress
- requestUrl
- userAgent
- webApp

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

### host

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
name	string		Specifies the name.

### remoteAddress

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
ip	string		Specifies the IP address.

Attribute name	Data type	Default value	Description
matchType	<ul style="list-style-type: none"> <li>lessThan</li> <li>equals</li> <li>greaterThan</li> <li>contains</li> <li>notContain</li> </ul>	contains	Specifies the match type. <b>lessThan</b> Less than <b>equals</b> Equals <b>greaterThan</b> Greater than <b>contains</b> Contains <b>notContain</b> Not contain

### requestUrl

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>equals</li> <li>contains</li> <li>notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
urlPattern	string		Specifies the URL pattern.

### userAgent

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
agent	string		Specifies the user agent
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>equals</li> <li>contains</li> <li>notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain

### webApp

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
name	string		Specifies the name.

## Authentication (authentication)

Controls the built-in authentication service configuration.

Attribute name	Data type	Default value	Description
allowHashtableLoginWithIdOnly	boolean	false	Allow an application to login with just an identity in the hashtable properties. Use this option only when you have applications that require this and have other means to validate the identity.
cacheEnabled	boolean	true	Enables the authentication cache.

## Feature Authorization Role Mapping (authorization-roles)

A collection of role names and mappings of the roles to users, groups, or special subjects

- security-role
  - group
  - special-subject
  - user

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

### security-role

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Role name.

### security-role > group

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		A group access ID in the general form group:realmName/groupUniqueId. A value will be generated if one is not specified.
id	string		A unique configuration ID.
name	string		Name of a group that has the security role.

#### security-role > special-subject

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
type	<ul style="list-style-type: none"> <li>• EVERYONE</li> <li>• ALL_AUTHENTICATED_USERS</li> </ul>		<p>One of the following special subject types: ALL_AUTHENTICATED_USERS, EVERYONE.</p> <p><b>EVERYONE</b> All users for every request, even if the request was not authenticated.</p> <p><b>ALL_AUTHENTICATED_USERS</b> All authenticated users.</p>

#### security-role > user

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		A user access ID in the general form user:realmName/userUniqueId. A value will be generated if one is not specified.
id	string		A unique configuration ID.
name	string		Name of a user who has the security role.

## z/OS Connect Authorization Interceptor (authorizationInterceptor)

Defines a z/OS Connect authorization interceptor.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
sequence	int Minimum: 0 Maximum: 2147483647	0	The sequence in which this interceptor should be processed with respect to other configured interceptors implementing z/OS Connect's com.ibm.wsspi.zos.connect.Interceptor Service Provider Interface (SPI).

## Basic User Registry (basicRegistry)

A simple XML-based user registry.

- group
  - member
- user

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
ignoreCaseForAuthentication	boolean	false	Allow case-insensitive user name authentication.
realm	string	BasicRegistry	The realm name represents the user registry.

### group

A group in a Basic User Registry.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Name of a group in a Basic User Registry.

### group > member

A member of a Basic User Registry group.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Name of a user in a Basic User Registry group.

### user

A user in a Basic User Registry.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
name	string		Name of a user in a Basic User Registry.
password	One way hashable, or reversably encoded password (string)		Password of a user in a Basic User Registry. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.

## Batch JMS Dispatcher (batchJmsDispatcher)

Configures the Batch JMS dispatcher.

- connectionFactory
  - connectionManager
  - containerAuthData
  - properties.wasJms
  - properties.wmqJms
  - recoveryAuthData
- queue
  - properties.wasJms
  - properties.wmqJms

Attribute name	Data type	Default value	Description
connectionFactoryRef	A reference to top level jmsConnectionFactory element (string).	batchConnectionFactory	The identifier of the JMS connection factory that the Batch dispatcher should use to obtain JMS connections.
id	string		A unique configuration ID.
queueRef	A reference to top level jmsQueue element (string).	batchJobSubmissionQueue	The identifier of the JMS queue that the Batch JMS dispatcher uses to send JMS messages.

### connectionFactory

The identifier of the JMS connection factory that the Batch dispatcher should use to obtain JMS connections.

false

Attribute name	Data type	Default value	Description
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a connection factory.

Attribute name	Data type	Default value	Description
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.
jndiName	string		JNDI name for a resource.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.

**connectionFactory > connectionManager**

Connection manager for a connection factory.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.

Attribute name	Data type	Default value	Description
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.

Attribute name	Data type	Default value	Description
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**connectionFactory > containerAuthData**

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

#### connectionFactory > properties.wasJms

A JMS connection factory is used to create connections to the associated JMS provider of JMS destinations, for both point-to-point and publish/subscribe messaging.

false

Attribute name	Data type	Default value	Description
busName	string	defaultBus	The name of a bus when connecting to the service integration bus in a full profile server.
clientID	string	clientID	The JMS client identifier needed for durable(and for shared non-durable) topic subscriptions on all connections. This identifier is required if the application is doing durable(and for shared non-durable) publish/subscribe messaging.
durableSubscriptionHome	string	defaultME	Durable subscription home defines ME name to which connection needs to be established.
nonPersistentMapping	<ul style="list-style-type: none"> <li>• BestEffortNonPersistent</li> <li>• ReliableNonPersistent</li> <li>• ExpressNonPersistent</li> </ul>	ExpressNonPersistent	<p>The reliability applied to Non-persistent JMS messages sent using this connection factory.</p> <p><b>BestEffortNonPersistent</b> BestEffortNonPersistent</p> <p><b>ReliableNonPersistent</b> ReliableNonPersistent</p> <p><b>ExpressNonPersistent</b> ExpressNonPersistent</p>
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.

Attribute name	Data type	Default value	Description
persistentMapping	<ul style="list-style-type: none"> <li>AssuredPersistent</li> <li>ReliablePersistent</li> </ul>	ReliablePersistent	<p>The reliability applied to persistent JMS messages sent using this connection factory.</p> <p><b>AssuredPersistent</b> AssuredPersistent</p> <p><b>ReliablePersistent</b> ReliablePersistent</p>
readAhead	<ul style="list-style-type: none"> <li>AlwaysOff</li> <li>Default</li> <li>AlwaysOn</li> </ul>	Default	<p>Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.</p> <p><b>AlwaysOff</b> AlwaysOff</p> <p><b>Default</b> Default</p> <p><b>AlwaysOn</b> AlwaysOn</p>
remoteServerAddress	string		<p>The remote server address that has triplets separated by a comma, with the syntax hostName:portNumber:chainName, used to connect to a bootstrap server. For example, Merlin:7276:BootstrapBasicMessaging. If hostName is not specified, the default is localhost. If portNumber is not specified, the default is 7276. If chainName is not specified, the default is BootstrapBasicMessaging. Refer to the information center for more information.</p>
shareDurableSubscription	string		Controls whether or not durable subscription can be shared across connections.
targetTransportChain	string		Transport chains specify the communication protocols that can be used to communicate with the service integration bus in a full profiles server.
temporaryQueueNamePrefix	string	temp	The prefix of up to twelve characters used for the temporary queues created by applications that use this queue connection factory.

Attribute name	Data type	Default value	Description
temporaryTopicNamePrefix	string	temp	The prefix of up to twelve characters used for the temporary topics created by applications that use this topic connection factory.
userName	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**connectionFactory > properties.wmqJms**  
 WebSphere MQ JMS connection factory  
 false

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	819	The coded character set identifier for a connection.
applicationName	string		The name by which an application is registered with the queue manager.
arbitraryProperties	string		Ability to specify properties not defined elsewhere
brokerCCSubQueue	string		The name of the queue from which a connection consumer receives nondurable subscription messages
brokerControlQueue	string		The name of the broker control queue
brokerPubQueue	string		The name of the queue where published messages are sent (the stream queue).
brokerQueueManager	string		The name of the queue manager on which the broker is running
brokerSubQueue	string		The name of the queue from which a nondurable message consumer receives messages
brokerVersion	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		The version of the broker being used  2      2 1      1
ccdtURL	string		A URL that identifies the name and location of the file containing the client channel definition table (CCDT) and specifies how the file can be accessed.

Attribute name	Data type	Default value	Description
channel	string		The name of the MQI channel to use.
cleanupInterval	A period of time with millisecond precision		The interval, in milliseconds, between background runs of the publish/subscribe cleanup utility. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
cleanupLevel	<ul style="list-style-type: none"> <li>• SAFE</li> <li>• FORCE</li> <li>• NONDUR</li> <li>• NONE</li> <li>• STRONG</li> </ul>	SAFE	<p>The cleanup level for a broker-based subscription store.</p> <p><b>SAFE</b> SAFE</p> <p><b>FORCE</b> FORCE</p> <p><b>NONDUR</b> NONDUR</p> <p><b>NONE</b> NONE</p> <p><b>STRONG</b> STRONG</p>
clientId	string		The client identifier for a connection
cloneSupport	<ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	DISABLED	<p>Whether two or more instances of the same durable topic subscriber can run simultaneously.</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DISABLED</b> DISABLED</p>
connectionNameList	string		A list of TCP/IP connection names (hostname(port))used for communications. ConnectionNameList supersedes the hostname and port properties.
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state.

Attribute name	Data type	Default value	Description
headerCompression	<ul style="list-style-type: none"> <li>• SYSTEM</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing header data on a connection</p> <p><b>SYSTEM</b> SYSTEM</p> <p><b>NONE</b> NONE</p>
hostName	string		<p>The host name or IP address of the system on which the queue manager resides. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.</p>
localAddress	string		<p>For a connection to a queue manager, this property specifies either or both of the following, (1) The local network interface to be used, (2) The local port, or range of local ports, to be used</p>
messageCompression	<ul style="list-style-type: none"> <li>• RLE</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing message data on a connection.</p> <p><b>RLE</b> RLE</p> <p><b>NONE</b> NONE</p>
messageSelection	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BROKER</li> </ul>	CLIENT	<p>Determines whether message selection is done by WebSphere MQ classes for JMS or by the broker.</p> <p><b>CLIENT</b> CLIENT</p> <p><b>BROKER</b> BROKER</p>
password	Reversably encoded password (string)		<p>The default password to use when creating a connection to the queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)</p>

Attribute name	Data type	Default value	Description						
pollingInterval	A period of time with millisecond precision		If each message listener within a session has no suitable message on its queue, this value is the maximum interval, in milliseconds, that elapses before each message listener tries again to get a message from its queue. If it frequently happens that no suitable message is available for any of the message listeners in a session, consider increasing the value of this property. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.						
port	int Minimum: 1	1414	The port on which the queue manager listens. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.						
providerVersion	<ul style="list-style-type: none"> <li>• 7</li> <li>• 6</li> <li>• unspecified</li> </ul>	unspecified	<p>The version, release, modification level and fix pack of the queue manager to which the application intends to connect.</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; text-align: center;">7</td> <td style="width: 50%; text-align: center;">7</td> </tr> <tr> <td style="text-align: center;">6</td> <td style="text-align: center;">6</td> </tr> <tr> <td style="text-align: center;"><b>unspecified</b></td> <td style="text-align: center;">unspecified</td> </tr> </table>	7	7	6	6	<b>unspecified</b>	unspecified
7	7								
6	6								
<b>unspecified</b>	unspecified								
pubAckInterval	int Minimum: 0	25	The number of messages published by a publisher before WebSphere MQ classes for JMS requests an acknowledgment from the broker						
queueManager	string		The name of the queue manager to connect to						
receiveExit	string		Identifies a channel receive exit program, or a sequence of receive exit programs to be run in succession						

Attribute name	Data type	Default value	Description
receiveExitInit	string		The user data that is passed to channel receive exit programs when they are called
rescanInterval	A period of time with millisecond precision	5s	When a message consumer in the point-to-point domain uses a message selector to select which messages it wants to receive, WebSphere MQ classes for JMS searches the WebSphere MQ queue for suitable messages in the sequence determined by the <code>MsgDeliverySequence</code> attribute of the queue. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
securityExit	string		Identifies a channel security exit program
securityExitInit	string		The user data that is passed to a channel security exit program when it is called
sendCheckCount	int Minimum: 0		The number of send calls to allow between checking for asynchronous put errors, within a single non-transacted JMS session.
sendExit	string		Identifies a channel send exit program, or a sequence of send exit programs to be run in succession.
sendExitInit	string		The user data that is passed to channel send exit programs when they are called.
shareConvAllowed	boolean	true	Whether a client connection can share its socket with other top-level JMS connections from the same process to the same queue manager, if the channel definitions match
sparseSubscriptions	boolean	false	Controls the message retrieval policy of a <code>TopicSubscriber</code> object.

Attribute name	Data type	Default value	Description
sslCertStores	string		The Lightweight Directory Access Protocol (LDAP) servers that hold certificate revocation lists (CRLs) for use on an SSL connection.
sslCipherSuite	string		The CipherSuite to use for an SSL connection.
sslFipsRequired	boolean		Whether an SSL connection must use a CipherSuite that is supported by the IBM Java JSSE FIPS provider (IBMJSSEFIPS).
sslPeerName	string		For an SSL connection, a template that is used to check the distinguished name in the digital certificate provided by the queue manager.
sslResetCount	int Minimum: 0 Maximum: 999999999	0	The total number of bytes sent and received by an SSL connection before the secret keys used by SSL are renegotiated.
statusRefreshInterval	A period of time with millisecond precision	1m	The interval, in milliseconds, between refreshes of the long running transaction that detects when a subscriber loses its connection to the queue manager. This property is relevant only if subscription store has the value QUEUE. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
subscriptionStore	<ul style="list-style-type: none"> <li>• MIGRATE</li> <li>• BROKER</li> <li>• QUEUE</li> </ul>	BROKER	<p>Determines where WebSphere MQ classes for JMS stores persistent data about active subscriptions.</p> <p><b>MIGRATE</b> MIGRATE</p> <p><b>BROKER</b> BROKER</p> <p><b>QUEUE</b> QUEUE</p>

Attribute name	Data type	Default value	Description
targetClientMatching	boolean	true	Whether a reply message, sent to the queue identified by the JMSReplyTo header field of an incoming message, has an MQRFH2 header only if the incoming message has an MQRFH2 header.
tempQPrefix	string		The prefix that is used to form the name of a WebSphere MQ dynamic queue.
tempTopicPrefix	string		When creating temporary topics, JMS generates a topic string of the form TEMP/TEMPTOPICPREFIX/unique_id, or if this property is left with the default value, just TEMP/unique_id. Specifying a non-empty TEMPTOPICPREFIX allows specific model queues to be defined for creating the managed queues for subscribers to temporary topics created under this connection.
temporaryModel	string		The name of the model queue from which JMS temporary queues are created. SYSTEM.JMS.TEMPQ.MODEL can be used by the JMS Layer to create queues which accept persistent messages, as the default value cannot. SYSTEM.DEFAULT.MODEL.QUEUE can be opened only once. SYSTEM.JMS.TEMPQ.MODEL can be opened more than once. SYSTEM.DEFAULT.MODEL.QUEUE is deprecated.
transportType	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BINDINGS</li> </ul>	CLIENT	Whether a connection to a queue manager uses client mode or bindings mode.  <b>CLIENT</b> CLIENT  <b>BINDINGS</b> BINDINGS

Attribute name	Data type	Default value	Description
userName	string		The default user name to use when creating a connection to a queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)
wildcardFormat	<ul style="list-style-type: none"> <li>• CHAR</li> <li>• TOPIC</li> </ul>	TOPIC	Which version of wildcard syntax is to be used.  <b>CHAR</b> CHAR <b>TOPIC</b> TOPIC

**connectionFactory > recoveryAuthData**

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

**queue**

The identifier of the JMS queue that the Batch JMS dispatcher uses to send JMS messages.

false

Attribute name	Data type	Default value	Description
jndiName	string		JNDI name for a resource.

**queue > properties.wasJms**

The name of the queue that this JMS queue is assigned to.

false

Attribute name	Data type	Default value	Description
deliveryMode	<ul style="list-style-type: none"> <li>• NonPersistent</li> <li>• Application</li> <li>• Persistent</li> </ul>	Application	<p>The delivery mode for messages sent to this destination. This controls the persistence of messages on this destination.</p> <p><b>NonPersistent</b> NonPersistent</p> <p><b>Application</b> Application</p> <p><b>Persistent</b> Persistent</p>
priority	int  Minimum: 0  Maximum: 9		<p>The relative priority for messages sent to this destination, in the range 0 to 9, with 0 as the lowest priority and 9 as the highest priority.</p>
queueName	string	Default.Queue	The name of the associated Queue
readAhead	<ul style="list-style-type: none"> <li>• AlwaysOff</li> <li>• AsConnection</li> <li>• AlwaysOn</li> </ul>	AsConnection	<p>Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.</p> <p><b>AlwaysOff</b> AlwaysOff</p> <p><b>AsConnection</b> AsConnection</p> <p><b>AlwaysOn</b> AlwaysOn</p>
timeToLive	A period of time with second precision	0s	<p>The default time in milliseconds from its dispatch time that the system must keep the messages live in the destination. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>

```
queue > properties.wmqJms
WebSphere MQ JMS Queue
false
```

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	1208	The coded character set ID to be used for a connection or destination
arbitraryProperties	string		Ability to specify properties not defined elsewhere
baseQueueManagerName	string		Queue Manager name that has this queue defined on it
baseQueueName	string		Name of the Queue on the Queue Manager
encoding	string	NATIVE	How numeric data in the body of a message is represented when the message is sent to this destination. The property specifies the representation of binary integers, packed decimal integers, and floating point numbers.
expiry	string	APP	The period after which messages at a destination expire
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state
persistence	<ul style="list-style-type: none"> <li>• APP</li> <li>• QDEF</li> <li>• HIGH</li> <li>• NON</li> <li>• PERS</li> </ul>	APP	The persistence of messages sent to a destination <b>APP</b> APP <b>QDEF</b> QDEF <b>HIGH</b> HIGH <b>NON</b> NON <b>PERS</b> PERS
priority	<ul style="list-style-type: none"> <li>• 3</li> <li>• 2</li> <li>• 1</li> <li>• APP</li> <li>• 0</li> <li>• 7</li> <li>• 6</li> <li>• 5</li> <li>• QDEF</li> <li>• 4</li> <li>• 9</li> <li>• 8</li> </ul>	APP	The priority for messages sent to a destination <b>3</b> 3 <b>2</b> 2 <b>1</b> 1 <b>APP</b> APP <b>0</b> 0 <b>7</b> 7 <b>6</b> 6 <b>5</b> 5 <b>QDEF</b> QDEF <b>4</b> 4 <b>9</b> 9 <b>8</b> 8

Attribute name	Data type	Default value	Description
putAsyncAllowed	<ul style="list-style-type: none"> <li>ENABLED</li> <li>DESTINATION</li> <li>DISABLED</li> </ul>	DESTINATION	<p>Whether message producers are allowed to use asynchronous puts to send messages to this destination</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DESTINATION</b> DESTINATION</p> <p><b>DISABLED</b> DISABLED</p>
readAheadAllowed	<ul style="list-style-type: none"> <li>ENABLED</li> <li>DESTINATION</li> <li>DISABLED</li> </ul>	DESTINATION	<p>Whether the MDB is allowed to use read ahead to get nonpersistent messages from the destination into an internal buffer before receiving them</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DESTINATION</b> DESTINATION</p> <p><b>DISABLED</b> DISABLED</p>
readAheadClosePolicy	<ul style="list-style-type: none"> <li>CURRENT</li> <li>ALL</li> </ul>	ALL	<p>What happens to messages in the internal read ahead buffer when the MDB is stopped by the administrator.</p> <p><b>CURRENT</b> CURRENT</p> <p><b>ALL</b> ALL</p>
receiveCCSID	<p>int</p> <p>Minimum: 0</p>		<p>Destination property that sets the target Coded character set identifier for queue manager message conversion. The value is ignored unless receive conversion is set to WMQ_RECEIVE_CONVERSION_QMG</p>
receiveConversion	<ul style="list-style-type: none"> <li>QMGR</li> <li>CLIENT_MSG</li> </ul>	CLIENT_MSG	<p>Destination property that determines if data conversion is going to be performed by the queue manager.</p> <p><b>QMGR</b> QMGR</p> <p><b>CLIENT_MSG</b> CLIENT_MSG</p>

Attribute name	Data type	Default value	Description
targetClient	<ul style="list-style-type: none"> <li>• JMS</li> <li>• MQ</li> </ul>	JMS	Whether the WebSphere MQ RFH2 format is used to exchange information with target applications  <b>JMS</b> JMS <b>MQ</b> MQ

## Batch JMS Events (batchJmsEvents)

Configure the Batch JMS events.

- connectionFactory
  - connectionManager
  - containerAuthData
  - properties.wasJms
  - properties.wmqJms
  - recoveryAuthData

Attribute name	Data type	Default value	Description
connectionFactoryRef	A reference to top level jmsConnectionFactory element (string).	batchConnectionFactory	The identifier of the JMS connection factory.
id	string		A unique configuration ID.

### connectionFactory

The identifier of the JMS connection factory.

false

Attribute name	Data type	Default value	Description
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a connection factory.
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.
jndiName	string		JNDI name for a resource.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.

### connectionFactory > connectionManager

Connection manager for a connection factory.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.

Attribute name	Data type	Default value	Description
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**connectionFactory > containerAuthData**

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

**connectionFactory > properties.wasJms**

A JMS connection factory is used to create connections to the associated JMS provider of JMS destinations, for both point-to-point and publish/subscribe messaging.

false

Attribute name	Data type	Default value	Description
busName	string	defaultBus	The name of a bus when connecting to the service integration bus in a full profile server.
clientID	string	clientID	The JMS client identifier needed for durable(and for shared non-durable) topic subscriptions on all connections. This identifier is required if the application is doing durable(and for shared non-durable) publish/subscribe messaging.
durableSubscriptionHome	string	defaultME	Durable subscription home defines ME name to which connection needs to be established.
nonPersistentMapping	<ul style="list-style-type: none"> <li>• BestEffortNonPersistent</li> <li>• ReliableNonPersistent</li> <li>• ExpressNonPersistent</li> </ul>	ExpressNonPersistent	The reliability applied to Non-persistent JMS messages sent using this connection factory.  <b>BestEffortNonPersistent</b> BestEffortNonPersistent  <b>ReliableNonPersistent</b> ReliableNonPersistent  <b>ExpressNonPersistent</b> ExpressNonPersistent

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
persistentMapping	<ul style="list-style-type: none"> <li>AssuredPersistent</li> <li>ReliablePersistent</li> </ul>	ReliablePersistent	<p>The reliability applied to persistent JMS messages sent using this connection factory.</p> <p><b>AssuredPersistent</b> AssuredPersistent</p> <p><b>ReliablePersistent</b> ReliablePersistent</p>
readAhead	<ul style="list-style-type: none"> <li>AlwaysOff</li> <li>Default</li> <li>AlwaysOn</li> </ul>	Default	<p>Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.</p> <p><b>AlwaysOff</b> AlwaysOff</p> <p><b>Default</b> Default</p> <p><b>AlwaysOn</b> AlwaysOn</p>
remoteServerAddress	string		<p>The remote server address that has triplets separated by a comma, with the syntax hostName:portNumber:chainName, used to connect to a bootstrap server. For example, Merlin:7276:BootstrapBasicMessaging. If hostName is not specified, the default is localhost. If portNumber is not specified, the default is 7276. If chainName is not specified, the default is BootstrapBasicMessaging. Refer to the information center for more information.</p>
shareDurableSubscription	string		Controls whether or not durable subscription can be shared across connections.
targetTransportChain	string		Transport chains specify the communication protocols that can be used to communicate with the service integration bus in a full profiles server.

Attribute name	Data type	Default value	Description
temporaryQueueNamePrefix	string	temp	The prefix of up to twelve characters used for the temporary queues created by applications that use this queue connection factory.
temporaryTopicNamePrefix	string	temp	The prefix of up to twelve characters used for the temporary topics created by applications that use this topic connection factory.
userName	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**connectionFactory > properties.wmqJms**  
 WebSphere MQ JMS connection factory  
 false

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	819	The coded character set identifier for a connection.
applicationName	string		The name by which an application is registered with the queue manager.
arbitraryProperties	string		Ability to specify properties not defined elsewhere
brokerCCSubQueue	string		The name of the queue from which a connection consumer receives nondurable subscription messages
brokerControlQueue	string		The name of the broker control queue
brokerPubQueue	string		The name of the queue where published messages are sent (the stream queue).
brokerQueueManager	string		The name of the queue manager on which the broker is running
brokerSubQueue	string		The name of the queue from which a nondurable message consumer receives messages
brokerVersion	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		The version of the broker being used  2        2 1        1

Attribute name	Data type	Default value	Description
ccdtURL	string		A URL that identifies the name and location of the file containing the client channel definition table (CCDT) and specifies how the file can be accessed.
channel	string		The name of the MQI channel to use.
cleanupInterval	A period of time with millisecond precision		The interval, in milliseconds, between background runs of the publish/subscribe cleanup utility. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
cleanupLevel	<ul style="list-style-type: none"> <li>• SAFE</li> <li>• FORCE</li> <li>• NONDUR</li> <li>• NONE</li> <li>• STRONG</li> </ul>	SAFE	<p>The cleanup level for a broker-based subscription store.</p> <p><b>SAFE</b> SAFE</p> <p><b>FORCE</b> FORCE</p> <p><b>NONDUR</b> NONDUR</p> <p><b>NONE</b> NONE</p> <p><b>STRONG</b> STRONG</p>
clientId	string		The client identifier for a connection
cloneSupport	<ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	DISABLED	<p>Whether two or more instances of the same durable topic subscriber can run simultaneously.</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DISABLED</b> DISABLED</p>
connectionNameList	string		A list of TCP/IP connection names (hostname(port)) used for communications. ConnectionNameList supersedes the hostname and port properties.

Attribute name	Data type	Default value	Description
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state.
headerCompression	<ul style="list-style-type: none"> <li>• SYSTEM</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing header data on a connection</p> <p><b>SYSTEM</b> SYSTEM</p> <p><b>NONE</b> NONE</p>
hostName	string		The host name or IP address of the system on which the queue manager resides. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.
localAddress	string		For a connection to a queue manager, this property specifies either or both of the following, (1) The local network interface to be used, (2) The local port, or range of local ports, to be used
messageCompression	<ul style="list-style-type: none"> <li>• RLE</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing message data on a connection.</p> <p><b>RLE</b> RLE</p> <p><b>NONE</b> NONE</p>
messageSelection	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BROKER</li> </ul>	CLIENT	<p>Determines whether message selection is done by WebSphere MQ classes for JMS or by the broker.</p> <p><b>CLIENT</b> CLIENT</p> <p><b>BROKER</b> BROKER</p>
password	Reversably encoded password (string)		The default password to use when creating a connection to the queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)

Attribute name	Data type	Default value	Description				
pollingInterval	A period of time with millisecond precision		If each message listener within a session has no suitable message on its queue, this value is the maximum interval, in milliseconds, that elapses before each message listener tries again to get a message from its queue. If it frequently happens that no suitable message is available for any of the message listeners in a session, consider increasing the value of this property. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.				
port	int Minimum: 1	1414	The port on which the queue manager listens. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.				
providerVersion	<ul style="list-style-type: none"> <li>• 7</li> <li>• 6</li> <li>• unspecified</li> </ul>	unspecified	<p>The version, release, modification level and fix pack of the queue manager to which the application intends to connect.</p> <table style="margin-left: 20px;"> <tr> <td style="padding-right: 20px;">7</td> <td>7</td> </tr> <tr> <td>6</td> <td>6</td> </tr> </table> <p><b>unspecified</b> unspecified</p>	7	7	6	6
7	7						
6	6						
pubAckInterval	int Minimum: 0	25	The number of messages published by a publisher before WebSphere MQ classes for JMS requests an acknowledgment from the broker				
queueManager	string		The name of the queue manager to connect to				
receiveExit	string		Identifies a channel receive exit program, or a sequence of receive exit programs to be run in succession				

Attribute name	Data type	Default value	Description
receiveExitInit	string		The user data that is passed to channel receive exit programs when they are called
rescanInterval	A period of time with millisecond precision	5s	When a message consumer in the point-to-point domain uses a message selector to select which messages it wants to receive, WebSphere MQ classes for JMS searches the WebSphere MQ queue for suitable messages in the sequence determined by the <code>MsgDeliverySequence</code> attribute of the queue. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
securityExit	string		Identifies a channel security exit program
securityExitInit	string		The user data that is passed to a channel security exit program when it is called
sendCheckCount	int Minimum: 0		The number of send calls to allow between checking for asynchronous put errors, within a single non-transacted JMS session.
sendExit	string		Identifies a channel send exit program, or a sequence of send exit programs to be run in succession.
sendExitInit	string		The user data that is passed to channel send exit programs when they are called.
shareConvAllowed	boolean	true	Whether a client connection can share its socket with other top-level JMS connections from the same process to the same queue manager, if the channel definitions match
sparseSubscriptions	boolean	false	Controls the message retrieval policy of a <code>TopicSubscriber</code> object.

Attribute name	Data type	Default value	Description
sslCertStores	string		The Lightweight Directory Access Protocol (LDAP) servers that hold certificate revocation lists (CRLs) for use on an SSL connection.
sslCipherSuite	string		The CipherSuite to use for an SSL connection.
sslFipsRequired	boolean		Whether an SSL connection must use a CipherSuite that is supported by the IBM Java JSSE FIPS provider (IBMJSSEFIPS).
sslPeerName	string		For an SSL connection, a template that is used to check the distinguished name in the digital certificate provided by the queue manager.
sslResetCount	int Minimum: 0 Maximum: 999999999	0	The total number of bytes sent and received by an SSL connection before the secret keys used by SSL are renegotiated.
statusRefreshInterval	A period of time with millisecond precision	1m	The interval, in milliseconds, between refreshes of the long running transaction that detects when a subscriber loses its connection to the queue manager. This property is relevant only if subscription store has the value QUEUE. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
subscriptionStore	<ul style="list-style-type: none"> <li>• MIGRATE</li> <li>• BROKER</li> <li>• QUEUE</li> </ul>	BROKER	<p>Determines where WebSphere MQ classes for JMS stores persistent data about active subscriptions.</p> <p><b>MIGRATE</b> MIGRATE</p> <p><b>BROKER</b> BROKER</p> <p><b>QUEUE</b> QUEUE</p>

Attribute name	Data type	Default value	Description
targetClientMatching	boolean	true	Whether a reply message, sent to the queue identified by the JMSReplyTo header field of an incoming message, has an MQRFH2 header only if the incoming message has an MQRFH2 header.
tempQPrefix	string		The prefix that is used to form the name of a WebSphere MQ dynamic queue.
tempTopicPrefix	string		When creating temporary topics, JMS generates a topic string of the form TEMP/TEMPTOPICPREFIX/unique_id, or if this property is left with the default value, just TEMP/unique_id. Specifying a non-empty TEMPTOPICPREFIX allows specific model queues to be defined for creating the managed queues for subscribers to temporary topics created under this connection.
temporaryModel	string		The name of the model queue from which JMS temporary queues are created. SYSTEM.JMS.TEMPQ.MODEL can be used by the JMS Layer to create queues which accept persistent messages, as the default value cannot. SYSTEM.DEFAULT.MODEL.QUEUE can be opened only once. SYSTEM.JMS.TEMPQ.MODEL can be opened more than once. SYSTEM.DEFAULT.MODEL.QUEUE is deprecated.
transportType	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BINDINGS</li> </ul>	CLIENT	Whether a connection to a queue manager uses client mode or bindings mode.  <b>CLIENT</b> CLIENT  <b>BINDINGS</b> BINDINGS

Attribute name	Data type	Default value	Description
userName	string		The default user name to use when creating a connection to a queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)
wildcardFormat	<ul style="list-style-type: none"> <li>• CHAR</li> <li>• TOPIC</li> </ul>	TOPIC	Which version of wildcard syntax is to be used.  <b>CHAR</b> CHAR <b>TOPIC</b> TOPIC

**connectionFactory > recoveryAuthData**

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## Batch JMS Executor (batchJmsExecutor)

Configures the Batch JMS executor.

- activationSpec
  - authData
  - properties.wasJms
  - properties.wmqJms
- queue
  - properties.wasJms
  - properties.wmqJms
- replyConnectionFactory
  - connectionManager
  - containerAuthData
  - properties.wasJms
  - properties.wmqJms
  - recoveryAuthData

Attribute name	Data type	Default value	Description
activationSpecRef	A reference to top level jmsActivationSpec element (string).	batchActivationSpec	The identifier of the JMS activation specification that the Batch executor uses to create JMS listeners.
id	string		A unique configuration ID.
queueRef	A reference to top level jmsQueue element (string).	batchJobSubmissionQueue	The identifier of the JMS queue that the Batch activation specification uses to listen for batch JMS messages.
replyConnectionFactoryRef	A reference to top level jmsConnectionFactory element (string).	batchConnectionFactory	The identifier of the JMS connection factory that the Batch executor should use to obtain JMS connections.

### activationSpec

The identifier of the JMS activation specification that the Batch executor uses to create JMS listeners.

false

Attribute name	Data type	Default value	Description
authDataRef	A reference to top level authData element (string).		Default authentication data for an activation specification.
maxEndpoints	int Minimum: 0	500	The maximum number of endpoints to dispatch to.

### activationSpec > authData

Default authentication data for an activation specification.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

### activationSpec > properties.wasJms

A JMS activation specification is associated with one or more message-driven beans and provides the configuration necessary for them to receive messages.

false

Attribute name	Data type	Default value	Description
acknowledgeMode	<ul style="list-style-type: none"> <li>Dups-ok-acknowledge</li> <li>Auto-acknowledge</li> </ul>	Auto-acknowledge	<p>The acknowledge mode indicates how a message received by a message-driven bean should be acknowledged.</p> <p><b>Dups-ok-acknowledge</b> Dups-ok-acknowledge</p> <p><b>Auto-acknowledge</b> Auto-acknowledge</p>
busName	string	defaultBus	The name of a bus when connecting to the service integration bus in a full profile server.
clientId	string		The JMS client identifier needed for durable(and for shared non-durable) topic subscriptions on all connections. This identifier is required if the application is doing durable(and for shared non-durable) publish/subscribe messaging.
connectionFactoryLookup	string		This property can be used to specify the lookup name of an administratively-defined <code>javax.jms.ConnectionFactory</code> , <code>javax.jms.QueueConnectionFactory</code> or <code>javax.jms.TopicConnectionFactory</code> object that is used to connect to the JMS provider from which the endpoint (message-driven bean) can receive messages.
destination	string		Reference to a JMS destination
destinationLookup	string		This property can be used to specify the lookup name of the administratively-defined <code>javax.jms.Queue</code> or <code>javax.jms.Topic</code> objects that define the JMS queue or topic from which the endpoint (message-driven bean) can receive messages.
destinationRef	A reference to top level adminObject element (string).		Reference to a JMS destination

Attribute name	Data type	Default value	Description
destinationType	<ul style="list-style-type: none"> <li>javax.jms.Topic</li> <li>javax.jms.Queue</li> </ul>	javax.jms.Queue	<p>The type of the destination, which is javax.jms.Queue or javax.jms.Topic.</p> <p><b>javax.jms.Topic</b> javax.jms.Topic</p> <p><b>javax.jms.Queue</b> javax.jms.Queue</p>
maxBatchSize	int Minimum: 1 Maximum: 2147483647		The maximum number of messages received from the messaging engine in a single batch.
maxConcurrency	int Minimum: 1 Maximum: 2147483647	5	The maximum number of endpoints to which the messages are delivered concurrently. The increase in the number can improve the performance, but it also increases the number of threads that are in use at the specified time. If the message order must be retained for all the failed deliveries, set the maximum concurrent endpoints value to 1.
messageSelector	string		The JMS message selector used to determine which messages the message-driven bean receives. The value is a string that is used to select a subset of the available messages.
readAhead	<ul style="list-style-type: none"> <li>AlwaysOff</li> <li>Default</li> <li>AlwaysOn</li> </ul>	Default	<p>Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.</p> <p><b>AlwaysOff</b> AlwaysOff</p> <p><b>Default</b> Default</p> <p><b>AlwaysOn</b> AlwaysOn</p>

Attribute name	Data type	Default value	Description
remoteServerAddress	string		The remote server address that has triplets separated by a comma, with the syntax <code>hostName:portNumber:chainName</code> , used to connect to a bootstrap server. For example, <code>Merlin:7276:BootstrapBasicMessaging</code> . If <code>hostName</code> is not specified, the default is <code>localhost</code> . If <code>portNumber</code> is not specified, the default is <code>7276</code> . If <code>chainName</code> is not specified, the default is <code>BootstrapBasicMessaging</code> . Refer to the information center for more information.
retryInterval	A period of time with second precision	30s	The delay (in seconds) between attempts to connect to a messaging engine, both for the initial connection, and any subsequent attempts to establish a better connection. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as <code>30s</code> . You can include multiple values in a single entry. For example, <code>1m30s</code> is equivalent to 90 seconds.
shareDurableSubscription	string		Controls whether or not durable subscription can be shared across connections.
subscriptionDurability	<ul style="list-style-type: none"> <li>• DurableShared</li> <li>• Durable</li> <li>• NonDurable</li> <li>• NonDurableShared</li> </ul>	NonDurable	Type of MS topic subscription. The value can be any of following values: Durable DurableShared NonDurable NonDurableShared <b>DurableShared</b> DurableShared <b>Durable</b> Durable <b>NonDurable</b> NonDurable <b>NonDurableShared</b> NonDurableShared

Attribute name	Data type	Default value	Description
subscriptionName	string		The subscription name needed for durable(and for shared non-durable). Required field when using a durable(and for shared non-durable) topic subscription.This subscription name must be unique within a given client identifier.
targetTransportChain	<ul style="list-style-type: none"> <li>InboundSecureMessaging</li> <li>InboundBasicMessaging</li> </ul>	InboundBasicMessaging	<p>Transport chains specify the communication protocols that can be used to communicate with the service integration bus in a full profiles server.</p> <p><b>InboundSecureMessaging</b> InboundSecureMessaging</p> <p><b>InboundBasicMessaging</b> InboundBasicMessaging</p>

**activationSpec > properties.wmqJms**  
 WebSphere MQ JMS activation specification  
 false

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	819	The coded character set identifier for a connection.
applicationName	string		The name by which an application is registered with the queue manager.
brokerCCDurSubQueue	string		The name of the queue from which non-durable subscription messages are retrieved for a ConnectionConsumer
brokerCCSubQueue	string		The name of the queue from which a connection consumer receives nondurable subscription messages
brokerControlQueue	string		The name of the broker control queue
brokerPubQueue	string		The name of the queue where published messages are sent (the stream queue)
brokerQueueManager	string		The name of the queue manager on which the broker is running

Attribute name	Data type	Default value	Description
brokerSubQueue	string		The name of the queue from which a nondurable message consumer receives messages
brokerVersion	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>The version of the broker being used</p> <p><b>2</b>      2</p> <p><b>1</b>      1</p>
ccdtURL	string		A URL that identifies the name and location of the file containing the client channel definition table (CCDT) and specifies how the file can be accessed.
channel	string	SYSTEM.DEF.SVRCONN	The name of the MQI channel to use.
cleanupInterval	A period of time with millisecond precision		The interval, in milliseconds, between background runs of the publish/subscribe cleanup utility. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
cleanupLevel	<ul style="list-style-type: none"> <li>• SAFE</li> <li>• FORCE</li> <li>• NONDUR</li> <li>• NONE</li> <li>• STRONG</li> </ul>	SAFE	<p>The cleanup level for a broker-based subscription store.</p> <p><b>SAFE</b>    SAFE</p> <p><b>FORCE</b>            FORCE</p> <p><b>NONDUR</b>            NONDUR</p> <p><b>NONE</b>    NONE</p> <p><b>STRONG</b>            STRONG</p>
clientId	string		The client identifier for a connection

Attribute name	Data type	Default value	Description
cloneSupport	<ul style="list-style-type: none"> <li>ENABLED</li> <li>DISABLED</li> </ul>	DISABLED	<p>Whether two or more instances of the same durable topic subscriber can run simultaneously</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DISABLED</b> DISABLED</p>
connectionNameList	string		<p>A list of TCP/IP connection names (hostname(port)) used for communications. ConnectionNameList supersedes the hostname and port properties.</p>
destinationRef	A reference to top level adminObject element (string).		Destination
destinationType	<ul style="list-style-type: none"> <li>javax.jms.Topic</li> <li>javax.jms.Queue</li> </ul>	javax.jms.Queue	<p>The type of destination - javax.jms.Queue or javax.jms.Topic</p> <p><b>javax.jms.Topic</b> javax.jms.Topic</p> <p><b>javax.jms.Queue</b> javax.jms.Queue</p>
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state.
headerCompression	<ul style="list-style-type: none"> <li>SYSTEM</li> <li>NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing header data on a connection</p> <p><b>SYSTEM</b> SYSTEM</p> <p><b>NONE</b> NONE</p>
hostName	string	localhost	The host name or IP address of the system on which the queue manager resides. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.

Attribute name	Data type	Default value	Description
localAddress	string		For a connection to a queue manager, this property specifies either or both of the following, (1) The local network interface to be used, (2) The local port, or range of local ports, to be used
maxMessages	int Minimum: 0	1	The maximum number of messages that can be assigned to a server session at one time. If the activation spec is delivering messages to an MDB in an XA transaction, a value of 1 is used regardless of the setting of this property.
maxPoolDepth	int Minimum: 0	10	The maxPoolDepth property on the activation specification defines the number of available MDB (Message Driven Bean) instances. Decreasing the value of this property decreases the number of messages that can be delivered concurrently.
messageBatchSize	int Minimum: 0		Maximum number of messages to process in one batch.
messageCompression	<ul style="list-style-type: none"> <li>• RLE</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing message data on a connection</p> <p><b>RLE</b>    RLE <b>NONE</b>   NONE</p>
messageRetention	boolean		Whether the connection consumer keeps unwanted messages on the input queue
messageSelection	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BROKER</li> </ul>	CLIENT	<p>Determines whether message selection is done by WebSphere MQ classes for JMS or by the broker.</p> <p><b>CLIENT</b>           CLIENT <b>BROKER</b>           BROKER</p>

Attribute name	Data type	Default value	Description
messageSelector	string		Determines whether message selection is done by WebSphere MQ classes for JMS or by the broker. Message selection by the broker is not supported when brokerVersion has the value 1
pollingInterval	A period of time with millisecond precision	5s	If each message listener within a session has no suitable message on its queue, this value is the maximum interval, in milliseconds, that elapses before each message listener tries again to get a message from its queue. If it frequently happens that no suitable message is available for any of the message listeners in a session, consider increasing the value of this property. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
poolTimeout	A period of time with millisecond precision	5m	The time, in milliseconds, that an unused server session is held open in the server session pool before being closed due to inactivity. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
port	int Minimum: 1	1414	The port on which the queue manager listens. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.

Attribute name	Data type	Default value	Description
providerVersion	<ul style="list-style-type: none"> <li>7</li> <li>6</li> <li>unspecified</li> </ul>	unspecified	<p>The version, release, modification level and fix pack of the queue manager to which the application intends to connect.</p> <p>7      7</p> <p>6      6</p> <p><b>unspecified</b> unspecified</p>
queueManager	string		The name of the queue manager to connect to
receiveCCSID	int Minimum: 0	0	Destination property that sets the target Coded character set identifier for queue manager message conversion. The value is ignored unless receive conversion is set to WMQ_RECEIVE_CONVERSION_QMG
receiveConversion	<ul style="list-style-type: none"> <li>QMGR</li> <li>CLIENT_MSG</li> </ul>	CLIENT_MSG	Destination property that determines if data conversion is going to be performed by the queue manager. <p><b>QMGR</b> QMGR</p> <p><b>CLIENT_MSG</b> CLIENT_MSG</p>
receiveExit	string		Identifies a channel receive exit program, or a sequence of receive exit programs to be run in succession
receiveExitInit	string		The user data that is passed to channel receive exit programs when they are called

Attribute name	Data type	Default value	Description
rescanInterval	A period of time with millisecond precision	5s	When a message consumer in the point-to-point domain uses a message selector to select which messages it wants to receive, WebSphere MQ classes for JMS searches the WebSphere MQ queue for suitable messages in the sequence determined by the <code>MsgDeliverySequence</code> attribute of the queue. When WebSphere MQ classes for JMS finds a suitable message and delivers it to the consumer, WebSphere MQ classes for JMS resumes the search for the next suitable message from its current position in the queue. WebSphere MQ classes for JMS continues to search the queue in this way until it reaches the end of the queue, or until the interval of time in milliseconds, as determined by the value of this property, has expired. In each case, WebSphere MQ classes for JMS returns to the beginning of the queue to continue its search, and a new time interval commences. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
securityExit	string		Identifies a channel security exit program
securityExitInit	string		The user data that is passed to a channel security exit program when it is called
sendExit	string		Identifies a channel send exit program, or a sequence of send exit programs to be run in succession

Attribute name	Data type	Default value	Description
sendExitInit	string		The user data that is passed to channel send exit programs when they are called
shareConvAllowed	boolean	true	Whether a client connection can share its socket with other top-level JMS connections from the same process to the same queue manager, if the channel definitions match
sparseSubscriptions	boolean	false	Controls the message retrieval policy of a TopicSubscriber object
sslCertStores	string		The Lightweight Directory Access Protocol (LDAP) servers that hold certificate revocation lists (CRLs) for use on an SSL connection
sslCipherSuite	string		The CipherSuite to use for an SSL connection
sslFipsRequired	boolean		Whether an SSL connection must use a CipherSuite that is supported by the IBM Java JSSE FIPS provider (IBMJSSEFIPS).
sslPeerName	string		For an SSL connection, a template that is used to check the distinguished name in the digital certificate provided by the queue manager
sslResetCount	int Minimum: 0 Maximum: 999999999	0	The total number of bytes sent and received by an SSL connection before the secret keys used by SSL are renegotiated
startTimeout	A period of time with millisecond precision	10s	Configures the time duration (in milliseconds) within which the execution must start. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
statusRefreshInterval	A period of time with millisecond precision	1m	The interval, in milliseconds, between refreshes of the long running transaction that detects when a subscriber loses its connection to the queue manager. This property is relevant only if subscription store has the value QUEUE. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
subscriptionDurability	<ul style="list-style-type: none"> <li>Durable</li> <li>NonDurable</li> </ul>		<p>Whether a durable or nondurable subscription is used to deliver messages to an MDB subscribing to the topic</p> <p><b>Durable</b> Durable</p> <p><b>NonDurable</b> NonDurable</p>
subscriptionName	string		The name of the durable subscription
subscriptionStore	<ul style="list-style-type: none"> <li>MIGRATE</li> <li>BROKER</li> <li>QUEUE</li> </ul>	BROKER	<p>Determines where WebSphere MQ classes for JMS stores persistent data about active subscriptions</p> <p><b>MIGRATE</b> MIGRATE</p> <p><b>BROKER</b> BROKER</p> <p><b>QUEUE</b> QUEUE</p>
transportType	<ul style="list-style-type: none"> <li>CLIENT</li> <li>BINDINGS</li> </ul>	CLIENT	<p>Whether a connection to a queue manager uses client mode or bindings mode.</p> <p><b>CLIENT</b> CLIENT</p> <p><b>BINDINGS</b> BINDINGS</p>
wildcardFormat	<ul style="list-style-type: none"> <li>CHAR</li> <li>TOPIC</li> </ul>	TOPIC	<p>Which version of wildcard syntax is to be used.</p> <p><b>CHAR</b> CHAR</p> <p><b>TOPIC</b> TOPIC</p>

## queue

The identifier of the JMS queue that the Batch activation specification uses to listen for batch JMS messages.

false

Attribute name	Data type	Default value	Description
jndiName	string		JNDI name for a resource.

## queue > properties.wasJms

The name of the queue that this JMS queue is assigned to.

false

Attribute name	Data type	Default value	Description
deliveryMode	<ul style="list-style-type: none"><li>NonPersistent</li><li>Application</li><li>Persistent</li></ul>	Application	The delivery mode for messages sent to this destination. This controls the persistence of messages on this destination.  <b>NonPersistent</b> NonPersistent  <b>Application</b> Application  <b>Persistent</b> Persistent
priority	int  Minimum: 0  Maximum: 9		The relative priority for messages sent to this destination, in the range 0 to 9, with 0 as the lowest priority and 9 as the highest priority.
queueName	string	Default.Queue	The name of the associated Queue
readAhead	<ul style="list-style-type: none"><li>AlwaysOff</li><li>AsConnection</li><li>AlwaysOn</li></ul>	AsConnection	Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.  <b>AlwaysOff</b> AlwaysOff  <b>AsConnection</b> AsConnection  <b>AlwaysOn</b> AlwaysOn

Attribute name	Data type	Default value	Description
timeToLive	A period of time with second precision	0s	The default time in milliseconds from its dispatch time that the system must keep the messages live in the destination. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

```

queue > properties.wmqJms
WebSphere MQ JMS Queue
false

```

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	1208	The coded character set ID to be used for a connection or destination
arbitraryProperties	string		Ability to specify properties not defined elsewhere
baseQueueManagerName	string		Queue Manager name that has this queue defined on it
baseQueueName	string		Name of the Queue on the Queue Manager
encoding	string	NATIVE	How numeric data in the body of a message is represented when the message is sent to this destination. The property specifies the representation of binary integers, packed decimal integers, and floating point numbers.
expiry	string	APP	The period after which messages at a destination expire
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state

Attribute name	Data type	Default value	Description
persistence	<ul style="list-style-type: none"> <li>• APP</li> <li>• QDEF</li> <li>• HIGH</li> <li>• NON</li> <li>• PERS</li> </ul>	APP	<p>The persistence of messages sent to a destination</p> <p><b>APP</b> APP  <b>QDEF</b> QDEF  <b>HIGH</b> HIGH  <b>NON</b> NON  <b>PERS</b> PERS</p>
priority	<ul style="list-style-type: none"> <li>• 3</li> <li>• 2</li> <li>• 1</li> <li>• APP</li> <li>• 0</li> <li>• 7</li> <li>• 6</li> <li>• 5</li> <li>• QDEF</li> <li>• 4</li> <li>• 9</li> <li>• 8</li> </ul>	APP	<p>The priority for messages sent to a destination</p> <p><b>3</b> 3  <b>2</b> 2  <b>1</b> 1  <b>APP</b> APP  <b>0</b> 0  <b>7</b> 7  <b>6</b> 6  <b>5</b> 5  <b>QDEF</b> QDEF  <b>4</b> 4  <b>9</b> 9  <b>8</b> 8</p>
putAsyncAllowed	<ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DESTINATION</li> <li>• DISABLED</li> </ul>	DESTINATION	<p>Whether message producers are allowed to use asynchronous puts to send messages to this destination</p> <p><b>ENABLED</b>  ENABLED  <b>DESTINATION</b>  DESTINATION  <b>DISABLED</b>  DISABLED</p>
readAheadAllowed	<ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DESTINATION</li> <li>• DISABLED</li> </ul>	DESTINATION	<p>Whether the MDB is allowed to use read ahead to get nonpersistent messages from the destination into an internal buffer before receiving them</p> <p><b>ENABLED</b>  ENABLED  <b>DESTINATION</b>  DESTINATION  <b>DISABLED</b>  DISABLED</p>

Attribute name	Data type	Default value	Description
readAheadClosePolicy	<ul style="list-style-type: none"> <li>CURRENT</li> <li>ALL</li> </ul>	ALL	What happens to messages in the internal read ahead buffer when the MDB is stopped by the administrator. <b>CURRENT</b> CURRENT <b>ALL</b> ALL
receiveCCSID	int Minimum: 0		Destination property that sets the target Coded character set identifier for queue manager message conversion. The value is ignored unless receive conversion is set to WMQ_RECEIVE_CONVERSION_QMGR
receiveConversion	<ul style="list-style-type: none"> <li>QMGR</li> <li>CLIENT_MSG</li> </ul>	CLIENT_MSG	Destination property that determines if data conversion is going to be performed by the queue manager. <b>QMGR</b> QMGR <b>CLIENT_MSG</b> CLIENT_MSG
targetClient	<ul style="list-style-type: none"> <li>JMS</li> <li>MQ</li> </ul>	JMS	Whether the WebSphere MQ RFH2 format is used to exchange information with target applications <b>JMS</b> JMS <b>MQ</b> MQ

### replyConnectionFactory

The identifier of the JMS connection factory that the Batch executor should user to obtain JMS connections.

false

Attribute name	Data type	Default value	Description
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a connection factory.
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.
jndiName	string		JNDI name for a resource.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.

**replyConnectionFactory > connectionManager**  
 Connection manager for a connection factory.  
 false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**replyConnectionFactory > containerAuthData**

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

**replyConnectionFactory > properties.wasJms**

A JMS connection factory is used to create connections to the associated JMS provider of JMS destinations, for both point-to-point and publish/subscribe messaging.

false

Attribute name	Data type	Default value	Description
busName	string	defaultBus	The name of a bus when connecting to the service integration bus in a full profile server.
clientID	string	clientID	The JMS client identifier needed for durable(and for shared non-durable) topic subscriptions on all connections. This identifier is required if the application is doing durable(and for shared non-durable) publish/subscribe messaging.
durableSubscriptionHome	string	defaultME	Durable subscription home defines ME name to which connection needs to be established.
nonPersistentMapping	<ul style="list-style-type: none"> <li>• BestEffortNonPersistent</li> <li>• ReliableNonPersistent</li> <li>• ExpressNonPersistent</li> </ul>	ExpressNonPersistent	<p>The reliability applied to Non-persistent JMS messages sent using this connection factory.</p> <p><b>BestEffortNonPersistent</b> BestEffortNonPersistent</p> <p><b>ReliableNonPersistent</b> ReliableNonPersistent</p> <p><b>ExpressNonPersistent</b> ExpressNonPersistent</p>

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
persistentMapping	<ul style="list-style-type: none"> <li>AssuredPersistent</li> <li>ReliablePersistent</li> </ul>	ReliablePersistent	<p>The reliability applied to persistent JMS messages sent using this connection factory.</p> <p><b>AssuredPersistent</b> AssuredPersistent</p> <p><b>ReliablePersistent</b> ReliablePersistent</p>
readAhead	<ul style="list-style-type: none"> <li>AlwaysOff</li> <li>Default</li> <li>AlwaysOn</li> </ul>	Default	<p>Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.</p> <p><b>AlwaysOff</b> AlwaysOff</p> <p><b>Default</b> Default</p> <p><b>AlwaysOn</b> AlwaysOn</p>
remoteServerAddress	string		<p>The remote server address that has triplets separated by a comma, with the syntax hostName:portNumber:chainName, used to connect to a bootstrap server. For example, Merlin:7276:BootstrapBasicMessaging. If hostName is not specified, the default is localhost. If portNumber is not specified, the default is 7276. If chainName is not specified, the default is BootstrapBasicMessaging. Refer to the information center for more information.</p>
shareDurableSubscription	string		Controls whether or not durable subscription can be shared across connections.
targetTransportChain	string		Transport chains specify the communication protocols that can be used to communicate with the service integration bus in a full profiles server.

Attribute name	Data type	Default value	Description
temporaryQueueNamePrefix	string	temp	The prefix of up to twelve characters used for the temporary queues created by applications that use this queue connection factory.
temporaryTopicNamePrefix	string	temp	The prefix of up to twelve characters used for the temporary topics created by applications that use this topic connection factory.
userName	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**replyConnectionFactory > properties.wmqJms**

WebSphere MQ JMS connection factory

false

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	819	The coded character set identifier for a connection.
applicationName	string		The name by which an application is registered with the queue manager.
arbitraryProperties	string		Ability to specify properties not defined elsewhere
brokerCCSubQueue	string		The name of the queue from which a connection consumer receives nondurable subscription messages
brokerControlQueue	string		The name of the broker control queue
brokerPubQueue	string		The name of the queue where published messages are sent (the stream queue).
brokerQueueManager	string		The name of the queue manager on which the broker is running
brokerSubQueue	string		The name of the queue from which a nondurable message consumer receives messages
brokerVersion	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		The version of the broker being used  <b>2</b> 2 <b>1</b> 1

Attribute name	Data type	Default value	Description
ccdtURL	string		A URL that identifies the name and location of the file containing the client channel definition table (CCDT) and specifies how the file can be accessed.
channel	string		The name of the MQI channel to use.
cleanupInterval	A period of time with millisecond precision		The interval, in milliseconds, between background runs of the publish/subscribe cleanup utility. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
cleanupLevel	<ul style="list-style-type: none"> <li>• SAFE</li> <li>• FORCE</li> <li>• NONDUR</li> <li>• NONE</li> <li>• STRONG</li> </ul>	SAFE	<p>The cleanup level for a broker-based subscription store.</p> <p><b>SAFE</b> SAFE</p> <p><b>FORCE</b> FORCE</p> <p><b>NONDUR</b> NONDUR</p> <p><b>NONE</b> NONE</p> <p><b>STRONG</b> STRONG</p>
clientId	string		The client identifier for a connection
cloneSupport	<ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	DISABLED	<p>Whether two or more instances of the same durable topic subscriber can run simultaneously.</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DISABLED</b> DISABLED</p>
connectionNameList	string		A list of TCP/IP connection names (hostname(port)) used for communications. ConnectionNameList supersedes the hostname and port properties.

Attribute name	Data type	Default value	Description
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state.
headerCompression	<ul style="list-style-type: none"> <li>• SYSTEM</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing header data on a connection</p> <p><b>SYSTEM</b> SYSTEM</p> <p><b>NONE</b> NONE</p>
hostName	string		The host name or IP address of the system on which the queue manager resides. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.
localAddress	string		For a connection to a queue manager, this property specifies either or both of the following, (1) The local network interface to be used, (2) The local port, or range of local ports, to be used
messageCompression	<ul style="list-style-type: none"> <li>• RLE</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing message data on a connection.</p> <p><b>RLE</b> RLE</p> <p><b>NONE</b> NONE</p>
messageSelection	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BROKER</li> </ul>	CLIENT	<p>Determines whether message selection is done by WebSphere MQ classes for JMS or by the broker.</p> <p><b>CLIENT</b> CLIENT</p> <p><b>BROKER</b> BROKER</p>
password	Reversably encoded password (string)		The default password to use when creating a connection to the queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)

Attribute name	Data type	Default value	Description				
pollingInterval	A period of time with millisecond precision		If each message listener within a session has no suitable message on its queue, this value is the maximum interval, in milliseconds, that elapses before each message listener tries again to get a message from its queue. If it frequently happens that no suitable message is available for any of the message listeners in a session, consider increasing the value of this property. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.				
port	int Minimum: 1	1414	The port on which the queue manager listens. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.				
providerVersion	<ul style="list-style-type: none"> <li>• 7</li> <li>• 6</li> <li>• unspecified</li> </ul>	unspecified	<p>The version, release, modification level and fix pack of the queue manager to which the application intends to connect.</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50px;">7</td> <td>7</td> </tr> <tr> <td>6</td> <td>6</td> </tr> </table> <p><b>unspecified</b> unspecified</p>	7	7	6	6
7	7						
6	6						
pubAckInterval	int Minimum: 0	25	The number of messages published by a publisher before WebSphere MQ classes for JMS requests an acknowledgment from the broker				
queueManager	string		The name of the queue manager to connect to				
receiveExit	string		Identifies a channel receive exit program, or a sequence of receive exit programs to be run in succession				

Attribute name	Data type	Default value	Description
receiveExitInit	string		The user data that is passed to channel receive exit programs when they are called
rescanInterval	A period of time with millisecond precision	5s	When a message consumer in the point-to-point domain uses a message selector to select which messages it wants to receive, WebSphere MQ classes for JMS searches the WebSphere MQ queue for suitable messages in the sequence determined by the <code>MsgDeliverySequence</code> attribute of the queue. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
securityExit	string		Identifies a channel security exit program
securityExitInit	string		The user data that is passed to a channel security exit program when it is called
sendCheckCount	int Minimum: 0		The number of send calls to allow between checking for asynchronous put errors, within a single non-transacted JMS session.
sendExit	string		Identifies a channel send exit program, or a sequence of send exit programs to be run in succession.
sendExitInit	string		The user data that is passed to channel send exit programs when they are called.
shareConvAllowed	boolean	true	Whether a client connection can share its socket with other top-level JMS connections from the same process to the same queue manager, if the channel definitions match
sparseSubscriptions	boolean	false	Controls the message retrieval policy of a <code>TopicSubscriber</code> object.

Attribute name	Data type	Default value	Description
sslCertStores	string		The Lightweight Directory Access Protocol (LDAP) servers that hold certificate revocation lists (CRLs) for use on an SSL connection.
sslCipherSuite	string		The CipherSuite to use for an SSL connection.
sslFipsRequired	boolean		Whether an SSL connection must use a CipherSuite that is supported by the IBM Java JSSE FIPS provider (IBMJSSEFIPS).
sslPeerName	string		For an SSL connection, a template that is used to check the distinguished name in the digital certificate provided by the queue manager.
sslResetCount	int Minimum: 0 Maximum: 999999999	0	The total number of bytes sent and received by an SSL connection before the secret keys used by SSL are renegotiated.
statusRefreshInterval	A period of time with millisecond precision	1m	The interval, in milliseconds, between refreshes of the long running transaction that detects when a subscriber loses its connection to the queue manager. This property is relevant only if subscription store has the value QUEUE. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
subscriptionStore	<ul style="list-style-type: none"> <li>• MIGRATE</li> <li>• BROKER</li> <li>• QUEUE</li> </ul>	BROKER	<p>Determines where WebSphere MQ classes for JMS stores persistent data about active subscriptions.</p> <p><b>MIGRATE</b> MIGRATE</p> <p><b>BROKER</b> BROKER</p> <p><b>QUEUE</b> QUEUE</p>

Attribute name	Data type	Default value	Description
targetClientMatching	boolean	true	Whether a reply message, sent to the queue identified by the JMSReplyTo header field of an incoming message, has an MQRFH2 header only if the incoming message has an MQRFH2 header.
tempQPrefix	string		The prefix that is used to form the name of a WebSphere MQ dynamic queue.
tempTopicPrefix	string		When creating temporary topics, JMS generates a topic string of the form TEMP/TEMPTOPICPREFIX/unique_id, or if this property is left with the default value, just TEMP/unique_id. Specifying a non-empty TEMPTOPICPREFIX allows specific model queues to be defined for creating the managed queues for subscribers to temporary topics created under this connection.
temporaryModel	string		The name of the model queue from which JMS temporary queues are created. SYSTEM.JMS.TEMPQ.MODEL can be used by the JMS Layer to create queues which accept persistent messages, as the default value cannot. SYSTEM.DEFAULT.MODEL.QUEUE can be opened only once. SYSTEM.JMS.TEMPQ.MODEL can be opened more than once. SYSTEM.DEFAULT.MODEL.QUEUE is deprecated.
transportType	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BINDINGS</li> </ul>	CLIENT	Whether a connection to a queue manager uses client mode or bindings mode.  <b>CLIENT</b> CLIENT  <b>BINDINGS</b> BINDINGS

Attribute name	Data type	Default value	Description
userName	string		The default user name to use when creating a connection to a queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)
wildcardFormat	<ul style="list-style-type: none"> <li>• CHAR</li> <li>• TOPIC</li> </ul>	TOPIC	Which version of wildcard syntax is to be used.  <b>CHAR</b> CHAR <b>TOPIC</b> TOPIC

**replyConnectionFactory > recoveryAuthData**  
 Authentication data for transaction recovery.  
 false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## Batch Job Logging (batchJobLogging)

Configures Batch job logging.

Attribute name	Data type	Default value	Description
enabled	boolean	true	Enables or disables batch job logging.
maxRecords	int Minimum: 0 Maximum: 2147483647	1000	The maximum number of log records per job log file before rolling over to the next file.

## Batch Persistence (batchPersistence)

Configures the Batch persistence store.

- jobStore
  - authData
  - dataSource
  - connectionManager
  - containerAuthData

- jaasLoginContextEntry
- jdbcDriver
  - library
    - file
    - fileset
    - folder
- properties
- properties.datadirect.sqlserver
- properties.db2.i.native
- properties.db2.i.toolbox
- properties.db2.jcc
- properties.derby.client
- properties.derby.embedded
- properties.informix
- properties.informix.jcc
- properties.microsoft.sqlserver
- properties.oracle
- properties.sybase
- recoveryAuthData

Attribute name	Data type	Default value	Description
jobStoreRef	A reference to top level databaseStore element (string).	defaultDatabaseStore	Persistent store for batch data.

### **jobStore**

Persistent store for batch data.

false

Attribute name	Data type	Default value	Description
authDataRef	A reference to top level authData element (string).		Authentication data for task scheduling, queries, and execution.
createTables	boolean	true	When set to true, database tables are created.
dataSourceRef	A reference to top level dataSource element (string).	DefaultDataSource	Data source that connects to the persistent store.

Attribute name	Data type	Default value	Description
keyGenerationStrategy	<ul style="list-style-type: none"> <li>• TABLE</li> <li>• SEQUENCE</li> <li>• IDENTITY</li> <li>• AUTO</li> </ul>	AUTO	<p>The preferred strategy for generating unique primary keys. If the selected strategy is not supported for the database, a different strategy might be used.</p> <p><b>TABLE</b> Use a database table to generate unique primary keys.</p> <p><b>SEQUENCE</b> Use a database sequence to generate unique primary keys.</p> <p><b>IDENTITY</b> Use a database identity column to generate unique primary keys.</p> <p><b>AUTO</b> Automatically select the strategy to generate unique primary keys.</p>
schema	string		Schema name with read and write access to the database tables.
tablePrefix	string	WLP	Name prefix for tables, sequences, and other database artifacts.

#### **jobStore > authData**

Authentication data for task scheduling, queries, and execution.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

#### **jobStore > dataSource**

Data source that connects to the persistent store.

false

Attribute name	Data type	Default value	Description
beginTranForResultSetScrolling	boolean	true	Attempt transaction enlistment when result set scrolling interfaces are used.
beginTranForVendorAPIs	boolean	true	Attempt transaction enlistment when vendor interfaces are used.
commitOrRollbackOnCleanup	<ul style="list-style-type: none"> <li>• commit</li> <li>• rollback</li> </ul>		<p>Determines how to clean up connections that might be in a database unit of work (AutoCommit=false) when the connection is closed or returned to the pool.</p> <p><b>commit</b> Clean up the connection by committing.</p> <p><b>rollback</b> Clean up the connection by rolling back.</p>
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a data source.
connectionSharing	<ul style="list-style-type: none"> <li>• MatchOriginalRequest</li> <li>• MatchCurrentState</li> </ul>	MatchOriginalRequest	<p>Specifies how connections are matched for sharing.</p> <p><b>MatchOriginalRequest</b> When sharing connections, match based on the original connection request.</p> <p><b>MatchCurrentState</b> When sharing connections, match based on the current state of the connection.</p>
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

Attribute name	Data type	Default value	Description
enableConnectionCasting	boolean	false	Indicates that connections obtained from the data source should be castable to interface classes that the JDBC vendor connection implementation implements. Enabling this option incurs additional overhead on each getConnection operation. If vendor JDBC interfaces are needed less frequently, it might be more efficient to leave this option disabled and use Connection.unwrap(interface) only where it is needed.
isolationLevel	<ul style="list-style-type: none"> <li>• TRANSACTION_REPEATABLE_READ</li> <li>• TRANSACTION_READ_COMMITTED</li> <li>• TRANSACTION_SERIALIZABLE</li> <li>• TRANSACTION_READ_UNCOMMITTED</li> <li>• TRANSACTION_SNAPSHOT</li> </ul>		<p>Default transaction isolation level.</p> <p><b>TRANSACTION_REPEATABLE_READ</b> Dirty reads and non-repeatable reads are prevented; phantom reads can occur.</p> <p><b>TRANSACTION_READ_COMMITTED</b> Dirty reads are prevented; non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SERIALIZABLE</b> Dirty reads, non-repeatable reads and phantom reads are prevented.</p> <p><b>TRANSACTION_READ_UNCOMMITTED</b> Dirty reads, non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SNAPSHOT</b> Snapshot isolation for Microsoft SQL Server JDBC Driver and DataDirect Connect for JDBC driver.</p>

Attribute name	Data type	Default value	Description
jaasLoginContextEntryRef	A reference to top level jaasLoginContextEntry element (string).		JAAS login context entry for authentication.
jdbcDriverRef	A reference to top level jdbcDriver element (string).		JDBC driver for a data source.
jndiName	string		JNDI name for a data source.
queryTimeout	A period of time with second precision		Default query timeout for SQL statements. In a JTA transaction, syncQueryTimeoutWithTransactionTimeout can override this default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.
statementCacheSize	int Minimum: 0	10	Maximum number of cached statements per connection.
supplementalJDBCTrace	boolean		Supplements the JDBC driver trace that is logged when JDBC driver trace is enabled in bootstrap.properties. JDBC driver trace specifications include: com.ibm.ws.database.logwriter, com.ibm.ws.db2.logwriter, com.ibm.ws.derby.logwriter, com.ibm.ws.informix.logwriter, com.ibm.ws.oracle.logwriter, com.ibm.ws.sqlserver.logwriter, com.ibm.ws.sybase.logwriter
syncQueryTimeoutWithTransactionTimeout	boolean	false	Use the time remaining (if any) in a JTA transaction as the default query timeout for SQL statements.
transactional	boolean	true	Enable participation in transactions that are managed by the application server.

Attribute name	Data type	Default value	Description
type	<ul style="list-style-type: none"> <li>javax.sql.DataSource</li> <li>javax.sql.XADataSource</li> <li>javax.sql.ConnectionPoolDataSource</li> </ul>		Type of data source. <b>javax.sql.DataSource</b> javax.sql.DataSource <b>javax.sql.XADataSource</b> javax.sql.XADataSource <b>javax.sql.ConnectionPoolDataSource</b> javax.sql.ConnectionPoolDataSource

**jobStore > dataSource > connectionManager**

Connection manager for a data source.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.

Attribute name	Data type	Default value	Description
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.

Attribute name	Data type	Default value	Description
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**jobStore > dataSource > containerAuthData**

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

**jobStore > dataSource > jaasLoginContextEntry**

JAAS login context entry for authentication.

false

Attribute name	Data type	Default value	Description
loginModuleRef	List of references to top level jaasLoginModule elements (comma-separated string).	hashtable,userNameAndPassword,certificate,trustID	Word certificate trustID of a JAAS login module.
name	string		Name of a JAAS configuration entry.

**jobStore > dataSource > jdbcDriver**

JDBC driver for a data source.

false

Attribute name	Data type	Default value	Description
javax.sql.ConnectionPoolDataSource	string		JDBC driver implementation of javax.sql.ConnectionPoolDataSource.
javax.sql.DataSource	string		JDBC driver implementation of javax.sql.DataSource.
javax.sql.XADataSource	string		JDBC driver implementation of javax.sql.XADataSource.
libraryRef	A reference to top level library element (string).		Identifies JDBC driver JARs and native files.

**jobStore > dataSource > jdbcDriver > library**

Identifies JDBC driver JARs and native files.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

**jobStore > dataSource > jdbcDriver > library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**jobStore > dataSource > jdbcDriver > library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**jobStore > dataSource > jdbcDriver > library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**jobStore > dataSource > properties**

List of JDBC vendor properties for the data source. For example, databaseName="dbname" serverName="localhost" portNumber="50000".

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database.
databaseName	string		JDBC driver property: databaseName.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
serverName	string		Server where the database is running.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**jobStore > dataSource > properties.datadirect.sqlserver**

Data source properties for the DataDirect Connect for JDBC driver for Microsoft SQL Server.

false

Attribute name	Data type	Default value	Description
JDBCBehavior	<ul style="list-style-type: none"> <li>• 1</li> <li>• 0</li> </ul>	0	JDBC driver property: JDBCBehavior. Values are: 0 (JDBC 4.0) or 1 (JDBC 3.0).  <b>1</b> JDBC 3.0 <b>0</b> JDBC 4.0
XATransactionGroup	string		JDBC driver property: XATransactionGroup.
XMLDescribeType	<ul style="list-style-type: none"> <li>• longvarbinary</li> <li>• longvarchar</li> </ul>		JDBC driver property: XMLDescribeType.  <b>longvarbinary</b> longvarbinary <b>longvarchar</b> longvarchar
accountingInfo	string		JDBC driver property: accountingInfo.
alternateServers	string		JDBC driver property: alternateServers.
alwaysReportTriggerResults	boolean		JDBC driver property: alwaysReportTriggerResults.
applicationName	string		JDBC driver property: applicationName.
authenticationMethod	<ul style="list-style-type: none"> <li>• ntlm</li> <li>• userIdPassword</li> <li>• kerberos</li> <li>• auto</li> </ul>		JDBC driver property: authenticationMethod.  <b>ntlm</b> ntlm <b>userIdPassword</b> userIdPassword <b>kerberos</b> kerberos <b>auto</b> auto
bulkLoadBatchSize	long		JDBC driver property: bulkLoadBatchSize.
bulkLoadOptions	long		JDBC driver property: bulkLoadOptions.
clientHostName	string		JDBC driver property: clientHostName.
clientUser	string		JDBC driver property: clientUser.

Attribute name	Data type	Default value	Description
codePageOverride	string		JDBC driver property: codePageOverride.
connectionRetryCount	int		JDBC driver property: connectionRetryCount.
connectionRetryDelay	A period of time with second precision		JDBC driver property: connectionRetryDelay. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
convertNull	int		JDBC driver property: convertNull.
databaseName	string		JDBC driver property: databaseName.
dateTimeInputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeInputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
dateTimeOutputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeOutputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
describeInputParameters	<ul style="list-style-type: none"> <li>• describeIfString</li> <li>• noDescribe</li> <li>• describeIfDateTime</li> <li>• describeAll</li> </ul>		JDBC driver property: describeInputParameters.  <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll

Attribute name	Data type	Default value	Description
describeOutputParameters	<ul style="list-style-type: none"> <li>describeIfString</li> <li>noDescribe</li> <li>describeIfDateTime</li> <li>describeAll</li> </ul>		JDBC driver property: describeOutputParameters. <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll
enableBulkLoad	boolean		JDBC driver property: enableBulkLoad.
enableCancelTimeout	boolean		JDBC driver property: enableCancelTimeout.
encryptionMethod	<ul style="list-style-type: none"> <li>loginSSL</li> <li>requestSSL</li> <li>SSL</li> <li>noEncryption</li> </ul>		JDBC driver property: encryptionMethod. <b>loginSSL</b> loginSSL <b>requestSSL</b> requestSSL <b>SSL</b> SSL <b>noEncryption</b> noEncryption
failoverGranularity	<ul style="list-style-type: none"> <li>disableIntegrityCheck</li> <li>atomicWithRepositioning</li> <li>nonAtomic</li> <li>atomic</li> </ul>		JDBC driver property: failoverGranularity. <b>disableIntegrityCheck</b> disableIntegrityCheck <b>atomicWithRepositioning</b> atomicWithRepositioning <b>nonAtomic</b> nonAtomic <b>atomic</b> atomic
failoverMode	<ul style="list-style-type: none"> <li>connect</li> <li>select</li> <li>extended</li> </ul>		JDBC driver property: failoverMode. <b>connect</b> connect <b>select</b> select <b>extended</b> extended
failoverPreconnect	boolean		JDBC driver property: failoverPreconnect.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
initializationString	string		JDBC driver property: initializationString.
insensitiveResultSetBufferSize	int		JDBC driver property: insensitiveResultSetBufferSize.

Attribute name	Data type	Default value	Description
javaDoubleToString	boolean		JDBC driver property: javaDoubleToString.
loadBalancing	boolean		JDBC driver property: loadBalancing.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
longDataCacheSize	int Minimum: -1		JDBC driver property: longDataCacheSize.
netAddress	string		JDBC driver property: netAddress.
packetSize	int Minimum: -1 Maximum: 128		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
queryTimeout	A period of time with second precision		JDBC driver property: queryTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
resultsetMetaDataOptions	int		JDBC driver property: resultSetMetaDataOptions.
selectMethod	<ul style="list-style-type: none"> <li>• direct</li> <li>• cursor</li> </ul>		JDBC driver property: selectMethod.  <b>direct</b> direct <b>cursor</b> cursor
serverName	string	localhost	Server where the database is running.
snapshotSerializable	boolean		JDBC driver property: snapshotSerializable.

Attribute name	Data type	Default value	Description
spyAttributes	string		JDBC driver property: spyAttributes.
stringInputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringInputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
stringOutputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringOutputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
suppressConnectionWarnings	boolean		JDBC driver property: suppressConnectionWarnings.
transactionMode	<ul style="list-style-type: none"> <li>explicit</li> <li>implicit</li> </ul>		JDBC driver property: transactionMode. <b>explicit</b> explicit <b>implicit</b> implicit
truncateFractionalSeconds	boolean		JDBC driver property: truncateFractionalSeconds.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
useServerSideUpdatableCursors	boolean		JDBC driver property: useServerSideUpdatableCursors.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
validateServerCertificate	boolean		JDBC driver property: validateServerCertificate.

### jobStore > dataSource > properties.db2.i.native

Data source properties for the IBM DB2 for i Native JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>read only</li> <li>all</li> <li>read call</li> </ul>	all	JDBC driver property: access. <b>read only</b> read only <b>all</b> all <b>read call</b> read call

Attribute name	Data type	Default value	Description
autoCommit	boolean	true	JDBC driver property: autoCommit.
batchStyle	<ul style="list-style-type: none"> <li>• 2.1</li> <li>• 2.0</li> </ul>	2.0	JDBC driver property: batchStyle. <b>2.1</b> 2.1 <b>2.0</b> 2.0
behaviorOverride	int		JDBC driver property: behaviorOverride.
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive
dataTruncation	string	true	JDBC driver property: dataTruncation.
databaseName	string	*LOCAL	JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy
dateSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		JDBC driver property: dateSeparator. <b>\,</b> The comma character (,). <b>b</b> The character b <b>.</b> The period character (.). <b>/</b> The forward slash character (/). <b>-</b> The dash character (-).
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		JDBC driver property: decimalSeparator. <b>\,</b> The comma character (,). <b>.</b> The period character (.).
directMap	boolean	true	JDBC driver property: directMap.
doEscapeProcessing	boolean	true	JDBC driver property: doEscapeProcessing.
fullErrors	boolean		JDBC driver property: fullErrors.
libraries	string		JDBC driver property: libraries.
lobThreshold	int Maximum: 500000	0	JDBC driver property: lobThreshold.

Attribute name	Data type	Default value	Description
lockTimeout	A period of time with second precision	0	JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>• 31</li> <li>• 63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 63
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
networkProtocol	int		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
prefetch	boolean	true	JDBC driver property: prefetch.
queryOptimizeGoal	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>	2	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).  <b>2</b> *ALLIO <b>1</b> *FIRSTIO

Attribute name	Data type	Default value	Description
reuseObjects	boolean	true	JDBC driver property: reuseObjects.
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
systemNaming	boolean	false	JDBC driver property: systemNaming.
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat.  <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  \,    The comma character (,). <b>b</b> The character b :    The colon character (:). .    The period character (.).
trace	boolean		JDBC driver property: trace.
transactionTimeout	A period of time with second precision	0	JDBC driver property: transactionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateHex	<ul style="list-style-type: none"> <li>• binary</li> <li>• character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
useBlockInsert	boolean	false	JDBC driver property: useBlockInsert.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**jobStore > dataSource > properties.db2.i.toolbox**

Data source properties for the IBM DB2 for i Toolbox JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>• read only</li> <li>• all</li> <li>• read call</li> </ul>	all	JDBC driver property: access.  <b>read only</b> read only  <b>all</b> all  <b>read call</b> read call
behaviorOverride	int		JDBC driver property: behaviorOverride.
bidiImplicitReordering	boolean	true	JDBC driver property: bidiImplicitReordering.
bidiNumericOrdering	boolean	false	JDBC driver property: bidiNumericOrdering.
bidiStringType	int		JDBC driver property: bidiStringType.
bigDecimal	boolean	true	JDBC driver property: bigDecimal.
blockCriteria	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>	2	JDBC driver property: blockCriteria. Values are: 0 (no record blocking), 1 (block if FOR FETCH ONLY is specified), 2 (block if FOR UPDATE is specified).  <b>2</b> 2  <b>1</b> 1  <b>0</b> 0

Attribute name	Data type	Default value	Description
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> <li>• insensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive <b>insensitive</b> insensitive
dataCompression	boolean	true	JDBC driver property: dataCompression.
dataTruncation	boolean	true	JDBC driver property: dataTruncation.
databaseName	string		JDBC driver property: databaseName.
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy

Attribute name	Data type	Default value	Description
dateSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		JDBC driver property: dateSeparator. The space character ( ). \, The comma character (,). . The period character (.). / The forward slash character (/). - The dash character (-).
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		JDBC driver property: decimalSeparator. \, The comma character (,). . The period character (.).
driver	<ul style="list-style-type: none"> <li>• toolbox</li> <li>• native</li> </ul>	toolbox	JDBC driver property: driver. <b>toolbox</b> toolbox <b>native</b> native
errors	<ul style="list-style-type: none"> <li>• full</li> <li>• basic</li> </ul>	basic	JDBC driver property: errors. <b>full</b> full <b>basic</b> basic
extendedDynamic	boolean	false	JDBC driver property: extendedDynamic.
extendedMetaData	boolean	false	JDBC driver property: extendedMetaData.
fullOpen	boolean	false	JDBC driver property: fullOpen.
holdInputLocators	boolean	true	JDBC driver property: holdInputLocators.
holdStatements	boolean	false	JDBC driver property: holdStatements.
isolationLevelSwitchingSupport	boolean	false	JDBC driver property: isolationLevelSwitchingSupport.
keepAlive	boolean		JDBC driver property: keepAlive.
lazyClose	boolean	false	JDBC driver property: lazyClose.
libraries	string		JDBC driver property: libraries.

Attribute name	Data type	Default value	Description
lobThreshold	int Minimum: 0 Maximum: 16777216	0	JDBC driver property: lobThreshold.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>• 31</li> <li>• 63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 64
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
metaDataSource	int Minimum: 0 Maximum: 1	1	JDBC driver property: metaDataSource.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
naming	<ul style="list-style-type: none"> <li>• system</li> <li>• sql</li> </ul>	sql	JDBC driver property: naming.  <b>system</b> system <b>sql</b> sql
package	string		JDBC driver property: package.
packageAdd	boolean	true	JDBC driver property: packageAdd.
packageCCSID	<ul style="list-style-type: none"> <li>• 13488</li> <li>• 1200</li> </ul>	13488	JDBC driver property: packageCCSID. Values are: 1200 (UCS-2) or 13488 (UTF-16).  <b>13488</b> 13488 (UTF-16) <b>1200</b> 1200 (UCS-2)
packageCache	boolean	false	JDBC driver property: packageCache.

Attribute name	Data type	Default value	Description
packageCriteria	<ul style="list-style-type: none"> <li>default</li> <li>select</li> </ul>	default	JDBC driver property: packageCriteria. <b>default</b> default <b>select</b> select
packageError	<ul style="list-style-type: none"> <li>exception</li> <li>none</li> <li>warning</li> </ul>	warning	JDBC driver property: packageError. <b>exception</b> exception <b>none</b> none <b>warning</b> warning
packageLibrary	string	QGPL	JDBC driver property: packageLibrary.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
prefetch	boolean	true	JDBC driver property: prefetch.
prompt	boolean	false	JDBC driver property: prompt.
proxyServer	string		JDBC driver property: proxyServer.
qaqqiniLibrary	string		JDBC driver property: qaqqiniLibrary.
queryOptimizeGoal	int Minimum: 0 Maximum: 2	0	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).
receiveBufferSize	int Minimum: 1		JDBC driver property: receiveBufferSize.
remarks	<ul style="list-style-type: none"> <li>system</li> <li>sql</li> </ul>	system	JDBC driver property: remarks. <b>system</b> system <b>sql</b> sql
rollbackCursorHold	boolean	false	JDBC driver property: rollbackCursorHold.
savePasswordWhenSerialized	boolean	false	JDBC driver property: savePasswordWhenSerialized.
secondaryUrl	string		JDBC driver property: secondaryUrl.
secure	boolean	false	JDBC driver property: secure.
sendBufferSize	int Minimum: 1		JDBC driver property: sendBufferSize.

Attribute name	Data type	Default value	Description
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
soLinger	A period of time with second precision		JDBC driver property: soLinger. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
soTimeout	A period of time with millisecond precision		JDBC driver property: soTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
sort	<ul style="list-style-type: none"> <li>• hex</li> <li>• table</li> <li>• language</li> </ul>	hex	JDBC driver property: sort. <b>hex</b> hex <b>table</b> table <b>language</b> language
sortLanguage	string		JDBC driver property: sortLanguage.
sortTable	string		JDBC driver property: sortTable.
sortWeight	<ul style="list-style-type: none"> <li>• unqiue</li> <li>• shared</li> </ul>		JDBC driver property: sortWeight. <b>unqiue</b> unique <b>shared</b> shared
tcpNoDelay	boolean		JDBC driver property: tcpNoDelay.
threadUsed	boolean	true	JDBC driver property: threadUsed.

Attribute name	Data type	Default value	Description
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat. <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  The space character ( ). \, The comma character (,). : The colon character (:). . The period character (.).
toolboxTrace	<ul style="list-style-type: none"> <li>• diagnostic</li> <li>• information</li> <li>• conversion</li> <li>• error</li> <li>• thread</li> <li>• proxy</li> <li>• none</li> <li>• datastream</li> <li>• pcml</li> <li>• all</li> <li>• jdbc</li> <li>• warning</li> </ul>		JDBC driver property: toolboxTrace. <b>diagnostic</b> diagnostic <b>information</b> information <b>conversion</b> conversion <b>error</b> error <b>thread</b> thread <b>proxy</b> proxy <b>none</b> none <b>datastream</b> datastream <b>pcml</b> pcml <b>all</b> all <b>jdbc</b> jdbc <b>warning</b> warning
trace	boolean		JDBC driver property: trace.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateBoolean	boolean	true	JDBC driver property: translateBoolean.

Attribute name	Data type	Default value	Description
translateHex	<ul style="list-style-type: none"> <li>binary</li> <li>character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
trueAutoCommit	boolean	false	JDBC driver property: trueAutoCommit.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaLooselyCoupledSupport	int  Minimum: 0  Maximum: 1	0	JDBC driver property: xaLooselyCoupledSupport.

### jobStore > dataSource > properties.db2.jcc

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for DB2.

false

Attribute name	Data type	Default value	Description
activateDatabase	int		JDBC driver property: activateDatabase.
alternateGroupDatabaseName	string		JDBC driver property: alternateGroupDatabaseName.
alternateGroupPortNumber	string		JDBC driver property: alternateGroupPortNumber.
alternateGroupServerName	string		JDBC driver property: alternateGroupServerName.
blockingReadConnectionTimeout	A period of time with second precision		JDBC driver property: blockingReadConnectionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
clientAccountingInformation	string		JDBC driver property: clientAccountingInformation.
clientApplicationInformation	string		JDBC driver property: clientApplicationInformation.
clientRerouteAlternatePortNumber	string		JDBC driver property: clientRerouteAlternatePortNumber.
clientRerouteAlternateServerName	string		JDBC driver property: clientRerouteAlternateServerName.

Attribute name	Data type	Default value	Description
clientUser	string		JDBC driver property: clientUser.
clientWorkstation	string		JDBC driver property: clientWorkstation.
connectionCloseWithInFlightTransaction	Transaction • 1		JDBC driver property: connectionCloseWithInFlightTransaction. 2 CONNECTION_CLOSE_WITH_ROLLBACK 1 CONNECTION_CLOSE_WITH_EXCEPTION
currentAlternateGroupEntry	int		JDBC driver property: currentAlternateGroupEntry.
currentFunctionPath	string		JDBC driver property: currentFunctionPath.
currentLocaleLcCtype	string		JDBC driver property: currentLocaleLcCtype.
currentLockTimeout	A period of time with second precision		JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
currentPackagePath	string		JDBC driver property: currentPackagePath.
currentPackageSet	string		JDBC driver property: currentPackageSet.
currentSQLID	string		JDBC driver property: currentSQLID.
currentSchema	string		JDBC driver property: currentSchema.
cursorSensitivity	• 2 • 1 • 0		JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). 2 TYPE_SCROLL_ASENSITIVE 1 TYPE_SCROLL_SENSITIVE_DYNAMIC 0 TYPE_SCROLL_SENSITIVE_STATIC
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean	true	JDBC driver property: deferPrepares.

Attribute name	Data type	Default value	Description
driverType	<ul style="list-style-type: none"> <li>2</li> <li>4</li> </ul>	4	JDBC driver property: driverType. 2 Type 2 JDBC driver. 4 Type 4 JDBC driver.
enableAlternateGroupSeamlessACR	boolean		JDBC driver property: enableAlternateGroupSeamlessACR.
enableClientAffinitiesList	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableClientAffinitiesList. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableExtendedDescribe	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedDescribe. 2 NO 1 YES
enableExtendedIndicators	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedIndicators. 2 NO 1 YES
enableNamedParameterMarkers	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSeamlessFailover	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeInputStreams	boolean		JDBC driver property: fullyMaterializeInputStreams.
fullyMaterializeInputStreamsOnBatchExecution	<ul style="list-style-type: none"> <li>1</li> </ul>		JDBC driver property: fullyMaterializeInputStreamsOnBatchExecution. 2 NO 1 YES
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.

Attribute name	Data type	Default value	Description
implicitRollbackOption	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: implicitRollbackOption.</p> <p>2 IMPLICIT_ROLLBACK_OPTION_CLOSE</p> <p>1 IMPLICIT_ROLLBACK_OPTION_NO</p> <p>0 IMPLICIT_ROLLBACK_OPTION_NO</p>
interruptProcessingMode	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: interruptProcessingMode.</p> <p>2 INTERRUPT_PROCESSING_MODE_C</p> <p>1 INTERRUPT_PROCESSING_MODE_S</p> <p>0 INTERRUPT_PROCESSING_MODE_D</p>
keepAliveTimeOut	A period of time with second precision		<p>JDBC driver property: keepAliveTimeOut. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
keepDynamic	int		JDBC driver property: keepDynamic.
kerberosServerPrincipal	string		JDBC driver property: kerberosServerPrincipal.
loginTimeout	A period of time with second precision		<p>JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
maxConnCachedParamBufferSize	int		JDBC driver property: maxConnCachedParamBufferSize.
maxRetriesForClientReroute	int		JDBC driver property: maxRetriesForClientReroute.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	50000	Port on which to obtain database connections.
profileName	string		JDBC driver property: profileName.

Attribute name	Data type	Default value	Description
queryCloseImplicit	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: queryCloseImplicit. Values are: 1 (QUERY_CLOSE_IMPLICIT_YES) or 2 (QUERY_CLOSE_IMPLICIT_NO).</p> <p>2        QUERY_CLOSE_IMPLICIT_NO 1        QUERY_CLOSE_IMPLICIT_YES</p>
queryDataSize	<p>int</p> <p>Minimum: 4096</p> <p>Maximum: 65535</p>		JDBC driver property: queryDataSize.
queryTimeoutInterruptProcessingMode	<p>int</p> <ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: queryTimeoutInterruptProcessingMode.</p> <p>2        INTERRUPT_PROCESSING_MODE 1        INTERRUPT_PROCESSING_MODE</p>
readOnly	boolean		JDBC driver property: readOnly.
recordTemporalHistory	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: recordTemporalHistory.</p> <p>2        NO 1        YES</p>
resultSetHoldability	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2        CLOSE_CURSORS_AT_COMMIT 1        HOLD_CURSORS_OVER_COMMIT</p>
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2        CLOSE_CURSORS_AT_COMMIT 1        HOLD_CURSORS_OVER_COMMIT</p>
retrieveMessagesFromServerOnGetMessage	boolean	true	JDBC driver property: retrieveMessagesFromServerOnGetMessage.

Attribute name	Data type	Default value	Description
retryIntervalForClientReroute	A period of time with second precision		JDBC driver property: retryIntervalForClientReroute. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 18</li> <li>• 15</li> <li>• 9</li> <li>• 16</li> <li>• 13</li> <li>• 11</li> <li>• 12</li> </ul>		<p>JDBC driver property: securityMechanism. Values are:</p> <ul style="list-style-type: none"> <li>3 (CLEAR_TEXT_PASSWORD_SECURITY),</li> <li>4 (USER_ONLY_SECURITY),</li> <li>7 (ENCRYPTED_PASSWORD_SECURITY),</li> <li>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY),</li> <li>11 (KERBEROS_SECURITY),</li> <li>12 (ENCRYPTED_USER_AND_DATA_SECURITY),</li> <li>13 (ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY),</li> <li>15 (PLUGIN_SECURITY),</li> <li>16 (ENCRYPTED_USER_ONLY_SECURITY),</li> <li>18 (TLS_CLIENT_CERTIFICATE_SECURITY).</li> </ul> <p>3 CLEAR_TEXT_PASSWORD_SECURITY  7 ENCRYPTED_PASSWORD_SECURITY  4 USER_ONLY_SECURITY  18 TLS_CLIENT_CERTIFICATE_SECURITY  15 PLUGIN_SECURITY  9 ENCRYPTED_USER_AND_PASSWORD_SECURITY  16 ENCRYPTED_USER_ONLY_SECURITY  13 ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY  11 KERBEROS_SECURITY  12 ENCRYPTED_USER_AND_DATA_SECURITY</p>
sendDataAsIs	boolean		JDBC driver property: sendDataAsIs.
serverName	string	localhost	Server where the database is running.
sessionTimeZone	string		JDBC driver property: sessionTimeZone.
sqljCloseStmtsWithOpenResultSet	boolean		JDBC driver property: sqljCloseStmtsWithOpenResultSet.

Attribute name	Data type	Default value	Description
sqljEnableClassLoaderSpecificProfiles	boolean		JDBC driver property: sqljEnableClassLoaderSpecificProfiles.
sslConnection	boolean		JDBC driver property: sslConnection.
streamBufferSize	int		JDBC driver property: streamBufferSize.
stripTrailingZerosForDecimalNumbers	Numbers <ul style="list-style-type: none"> <li>• 1</li> </ul>		JDBC driver property: stripTrailingZerosForDecimalNumbers. 2 NO 1 YES
sysSchema	string		JDBC driver property: sysSchema.
timerLevelForQueryTimeOut	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• -1</li> </ul>		JDBC driver property: timerLevelForQueryTimeOut. 2 QUERYTIMEOUT_CONNECTION 1 QUERYTIMEOUT_STATEMENT_L -1 QUERYTIMEOUT_DISABLED
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceFileCount	int		JDBC driver property: traceFileCount.
traceFileSize	int		JDBC driver property: traceFileSize.
traceLevel	int	0	Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
traceOption	<ul style="list-style-type: none"> <li>• 1</li> <li>• 0</li> </ul>		JDBC driver property: traceOption 1 1 0 0

Attribute name	Data type	Default value	Description
translateForBitData	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: translateForBitData. 2 SERVER_ENCODING_REPRESENTATION 1 HEX_REPRESENTATION
updateCountForBatch	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: updateCountForBatch. 2 TOTAL_UPDATE_COUNT 1 NO_UPDATE_COUNT
useCachedCursor	boolean		JDBC driver property: useCachedCursor.
useIdentityValLocalForAutoGeneratedKeys	boolean		JDBC driver property: useIdentityValLocalForAutoGeneratedKeys.
useJDBC41DefinitionForGetColumns	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC41DefinitionForGetColumns. 2 NO 1 YES
useJDBC4ColumnNameAndLabelSemantics	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
useTransactionRedirect	boolean		JDBC driver property: useTransactionRedirect.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaNetworkOptimization	boolean		JDBC driver property: xaNetworkOptimization.

**jobStore > dataSource > properties.derby.client**

Data source properties for Derby Network Client JDBC driver.

false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1527	Port on which to obtain database connections.
retrieveMessageText	boolean	true	JDBC driver property: retrieveMessageText.
securityMechanism	<ul style="list-style-type: none"> <li>3</li> <li>7</li> <li>4</li> <li>9</li> <li>8</li> </ul>	3	<p>JDBC driver property: securityMechanism. Values are:</p> <p>3 (CLEAR_TEXT_PASSWORD_SECURITY),</p> <p>4 (USER_ONLY_SECURITY),</p> <p>7 (ENCRYPTED_PASSWORD_SECURITY),</p> <p>8 (STRONG_PASSWORD_SUBSTITUTE_SECURITY),</p> <p>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY)</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY</p> <p>7 ENCRYPTED_PASSWORD_SECURITY</p> <p>4 USER_ONLY_SECURITY</p> <p>9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p> <p>8 STRONG_PASSWORD_SUBSTITUTE_SECURITY</p>

Attribute name	Data type	Default value	Description
serverName	string	localhost	Server where the database is running.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		JDBC driver property: shutdownDatabase. <b>false</b> Do not shut down the database. <b>shutdown</b> Shut down the database when a connection is attempted.
ssl	<ul style="list-style-type: none"> <li>basic</li> <li>off</li> <li>peerAuthentication</li> </ul>		JDBC driver property: ssl. <b>basic</b> basic <b>off</b> off <b>peerAuthentication</b> peerAuthentication
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_XA_CALLS=2048, TRACE_ALL=-1.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**jobStore > dataSource > properties.derby.embedded**

Data source properties for Derby Embedded JDBC driver.

false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		<p>JDBC driver property: shutdownDatabase.</p> <p><b>false</b> Do not shut down the database.</p> <p><b>shutdown</b> Shut down the database when a connection is attempted.</p>
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

### jobStore > dataSource > properties.informix

Data source properties for the Informix JDBC driver.

false

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
ifxCLIENT_LOCALE	string		JDBC driver property: ifxCLIENT_LOCALE.
ifxCPMAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMInitPoolSize	int		JDBC driver property: ifxCPMInitPoolSize.
ifxCPMMaxConnections	int		JDBC driver property: ifxCPMMaxConnections.
ifxCPMMaxPoolSize	int		JDBC driver property: ifxCPMMaxPoolSize.
ifxCPMMinAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMMinAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMMinPoolSize	int		JDBC driver property: ifxCPMMinPoolSize.
ifxCPMServiceInterval	A period of time with millisecond precision		JDBC driver property: ifxCPMServiceInterval. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxDBANSIWARN	boolean		JDBC driver property: ifxDBANSIWARN.
ifxDBCENTURY	string		JDBC driver property: ifxDBCENTURY.
ifxDBDATE	string		JDBC driver property: ifxDBDATE.
ifxDBSPACETEMP	string		JDBC driver property: ifxDBSPACETEMP.

Attribute name	Data type	Default value	Description
ifxDBTEMP	string		JDBC driver property: ifxDBTEMP.
ifxDBTIME	string		JDBC driver property: ifxDBTIME.
ifxDBUPSPACE	string		JDBC driver property: ifxDBUPSPACE.
ifxDB_LOCALE	string		JDBC driver property: ifxDB_LOCALE.
ifxDELIMIDENT	boolean		JDBC driver property: ifxDELIMIDENT.
ifxENABLE_TYPE_CACHE	boolean		JDBC driver property: ifxENABLE_TYPE_CACHE.
ifxFET_BUF_SIZE	int		JDBC driver property: ifxFET_BUF_SIZE.
ifxGL_DATE	string		JDBC driver property: ifxGL_DATE.
ifxGL_DATETIME	string		JDBC driver property: ifxGL_DATETIME.
ifxIFXHOST	string	localhost	JDBC driver property: ifxIFXHOST.
ifxIFX_AUTOFREE	boolean		JDBC driver property: ifxIFX_AUTOFREE.
ifxIFX_DIRECTIVES	string		JDBC driver property: ifxIFX_DIRECTIVES.
ifxIFX_LOCK_MODE_WAIT	A period of time with second precision	2s	JDBC driver property: ifxIFX_LOCK_MODE_WAIT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxIFX_SOC_TIMEOUT	A period of time with millisecond precision		JDBC driver property: ifxIFX_SOC_TIMEOUT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxIFX_USEPUT	boolean		JDBC driver property: ifxIFX_USEPUT.

Attribute name	Data type	Default value	Description
ifxIFX_USE_STRENC	boolean		JDBC driver property: ifxIFX_USE_STRENC.
ifxIFX_XASPEC	string	y	JDBC driver property: ifxIFX_XASPEC.
ifxINFORMIXCONRETRY	int		JDBC driver property: ifxINFORMIXCONRETRY.
ifxINFORMIXCONTIME	A period of time with second precision		JDBC driver property: ifxINFORMIXCONTIME. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxINFORMIXOPCACHE	string		JDBC driver property: ifxINFORMIXOPCACHE.
ifxINFORMIXSTACKSIZE	int		JDBC driver property: ifxINFORMIXSTACKSIZE.
ifxJDBCTEMP	string		JDBC driver property: ifxJDBCTEMP.
ifxLDAP_IFXBASE	string		JDBC driver property: ifxLDAP_IFXBASE.
ifxLDAP_PASSWD	string		JDBC driver property: ifxLDAP_PASSWD.
ifxLDAP_URL	string		JDBC driver property: ifxLDAP_URL.
ifxLDAP_USER	string		JDBC driver property: ifxLDAP_USER.
ifxLOBCACHE	int		JDBC driver property: ifxLOBCACHE.
ifxNEWCODESET	string		JDBC driver property: ifxNEWCODESET.
ifxNEWLOCALE	string		JDBC driver property: ifxNEWLOCALE.
ifxNODEFDAC	string		JDBC driver property: ifxNODEFDAC.
ifxOPTCOMPIND	string		JDBC driver property: ifxOPTCOMPIND.
ifxOPTOFC	string		JDBC driver property: ifxOPTOFC.
ifxOPT_GOAL	string		JDBC driver property: ifxOPT_GOAL.
ifxPATH	string		JDBC driver property: ifxPATH.
ifxPDQPRIORITY	string		JDBC driver property: ifxPDQPRIORITY.

Attribute name	Data type	Default value	Description
ifxPLCONFIG	string		JDBC driver property: ifxPLCONFIG.
ifxPLOAD_LO_PATH	string		JDBC driver property: ifxPLOAD_LO_PATH.
ifxPROTOCOLTRACE	int		JDBC driver property: ifxPROTOCOLTRACE.
ifxPROTOCOLTRACEFILE	string		JDBC driver property: ifxPROTOCOLTRACEFILE.
ifxPROXY	string		JDBC driver property: ifxPROXY.
ifxPSORT_DBTEMP	string		JDBC driver property: ifxPSORT_DBTEMP.
ifxPSORT_NPROCS	boolean		JDBC driver property: ifxPSORT_NPROCS.
ifxSECURITY	string		JDBC driver property: ifxSECURITY.
ifxSQLH_FILE	string		JDBC driver property: ifxSQLH_FILE.
ifxSQLH_LOC	string		JDBC driver property: ifxSQLH_LOC.
ifxSQLH_TYPE	string		JDBC driver property: ifxSQLH_TYPE.
ifxSSLCONNECTION	string		JDBC driver property: ifxSSLCONNECTION.
ifxSTMT_CACHE	string		JDBC driver property: ifxSTMT_CACHE.
ifxTRACE	int		JDBC driver property: ifxTRACE.
ifxTRACEFILE	string		JDBC driver property: ifxTRACEFILE.
ifxTRUSTED_CONTEXT	string		JDBC driver property: ifxTRUSTED_CONTEXT.
ifxUSEV5SERVER	boolean		JDBC driver property: ifxUSEV5SERVER.
ifxUSE_DTENV	boolean		JDBC driver property: ifxUSE_DTENV.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
roleName	string		JDBC driver property: roleName.
serverName	string		Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**jobStore > dataSource > properties.informix.jcc**

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for Informix.

false

Attribute name	Data type	Default value	Description
DBANSIWARN	boolean		JDBC driver property: DBANSIWARN.
DBDATE	string		JDBC driver property: DBDATE.
DBPATH	string		JDBC driver property: DBPATH.
DBSPACETEMP	string		JDBC driver property: DBSPACETEMP.
DBTEMP	string		JDBC driver property: DBTEMP.
DBUPSPACE	string		JDBC driver property: DBUPSPACE.
DELIMIDENT	boolean		JDBC driver property: DELIMIDENT.
IFX_DIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_DIRECTIVES. <b>ON</b> ON <b>OFF</b> OFF
IFX_EXTDIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_EXTDIRECTIVES. <b>ON</b> ON <b>OFF</b> OFF
IFX_UPDDESC	string		JDBC driver property: IFX_UPDDESC.

Attribute name	Data type	Default value	Description
IFX_XASTDCOMPLIANCE_XAEND	<ul style="list-style-type: none"> <li>0</li> </ul>		JDBC driver property: IFX_XASTDCOMPLIANCE_XAEND. <b>1</b> 1 <b>0</b> 0
INFORMIXOPCACHE	string		JDBC driver property: INFORMIXOPCACHE.
INFORMIXSTACKSIZE	string		JDBC driver property: INFORMIXSTACKSIZE.
NODEFDAC	<ul style="list-style-type: none"> <li>yes</li> <li>no</li> </ul>		JDBC driver property: NODEFDAC. <b>yes</b> yes <b>no</b> no
OPTCOMPIND	<ul style="list-style-type: none"> <li>2</li> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTCOMPIND. <b>2</b> 2 <b>1</b> 1 <b>0</b> 0
OPTOFC	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTOFC. <b>1</b> 1 <b>0</b> 0
PDQPRIORITY	<ul style="list-style-type: none"> <li>HIGH</li> <li>LOW</li> <li>OFF</li> </ul>		JDBC driver property: PDQPRIORITY. <b>HIGH</b> HIGH <b>LOW</b> LOW <b>OFF</b> OFF
PSORT_DBTEMP	string		JDBC driver property: PSORT_DBTEMP.
PSORT_NPROCS	string Maximum: 10		JDBC driver property: PSORT_NPROCS.
STMT_CACHE	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: STMT_CACHE. <b>1</b> 1 <b>0</b> 0
currentLockTimeout	A period of time with second precision	2s	JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean		JDBC driver property: deferPrepares.
driverType	int	4	JDBC driver property: driverType.
enableNamedParameterMarkers	int		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO).
enableSeamlessFailover	int		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO).
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.
keepDynamic	int		JDBC driver property: keepDynamic.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
progressiveStreaming	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		JDBC driver property: progressiveStreaming. Values are: 1 (YES) or 2 (NO).  2      NO 1      YES
queryDataSize	int  Minimum: 4096  Maximum: 10485760		JDBC driver property: queryDataSize.

Attribute name	Data type	Default value	Description
resultSetHoldability	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
retrieveMessagesFromServerOnGetMessage	boolean	true	<p>JDBC driver property: retrieveMessagesFromServerOnGetMessage.</p>
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 9</li> </ul>		<p>JDBC driver property: securityMechanism. Values are: 3 (CLEAR_TEXT_PASSWORD_SECURITY), 4 (USER_ONLY_SECURITY), 7 (ENCRYPTED_PASSWORD_SECURITY), 9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY).</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY 7 ENCRYPTED_PASSWORD_SECURITY 4 USER_ONLY_SECURITY 9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p>
serverName	string	localhost	Server where the database is running.
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.

Attribute name	Data type	Default value	Description
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
useJDBC4ColumnNameAndLabelSemantics	boolean		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO).
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**jobStore > dataSource > properties.microsoft.sqlserver**  
Data source properties for Microsoft SQL Server JDBC Driver.

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database. Example: jdbc:sqlserver://localhost:1433;databaseName=myDB.
applicationIntent	<ul style="list-style-type: none"> <li>ReadOnly</li> <li>ReadWrite</li> </ul>		JDBC driver property: applicationIntent. <b>ReadOnly</b> ReadOnly <b>ReadWrite</b> ReadWrite
applicationName	string		JDBC driver property: applicationName.
authenticationScheme	<ul style="list-style-type: none"> <li>NativeAuthentication</li> <li>JavaKerberos</li> </ul>		JDBC driver property: authenticationScheme. <b>NativeAuthentication</b> NativeAuthentication <b>JavaKerberos</b> JavaKerberos

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
encrypt	boolean		JDBC driver property: encrypt.
failoverPartner	string		JDBC driver property: failoverPartner.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
instanceName	string		JDBC driver property: instanceName.
integratedSecurity	boolean		JDBC driver property: integratedSecurity.
lastUpdateCount	boolean		JDBC driver property: lastUpdateCount.
lockTimeout	A period of time with millisecond precision		JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
multiSubnetFailover	boolean		JDBC driver property: multiSubnetFailover.
packetSize	int Minimum: 512 Maximum: 32767		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.

Attribute name	Data type	Default value	Description
responseBuffering	<ul style="list-style-type: none"> <li>full</li> <li>adaptive</li> </ul>		JDBC driver property: responseBuffering. <b>full</b> full <b>adaptive</b> adaptive
selectMethod	<ul style="list-style-type: none"> <li>direct</li> <li>cursor</li> </ul>		JDBC driver property: selectMethod. <b>direct</b> direct <b>cursor</b> cursor
sendStringParametersAsUnicode	boolean	false	JDBC driver property: sendStringParametersAsUnicode.
sendTimeAsDatetime	boolean		JDBC driver property: sendTimeAsDatetime.
serverName	string	localhost	Server where the database is running.
trustServerCertificate	boolean		JDBC driver property: trustServerCertificate.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
workstationID	string		JDBC driver property: workstationID.
xopenStates	boolean		JDBC driver property: xopenStates.

**jobStore > dataSource > properties.oracle**

Data source properties for Oracle JDBC driver.

false

Attribute name	Data type	Default value	Description
ONSConfiguration	string		JDBC driver property: ONSConfiguration.
TNSEntryName	string		JDBC driver property: TNSEntryName.
URL	string		URL for connecting to the database. Examples: jdbc:oracle:thin:@//localhost:1521/sample or jdbc:oracle:oci:@//localhost:1521/sample.
connectionProperties	string		JDBC driver property: connectionProperties.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
driverType	<ul style="list-style-type: none"> <li>oci</li> <li>thin</li> </ul>	thin	JDBC driver property: driverType.  <b>oci</b> oci <b>thin</b> thin
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	string		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1521	Port on which to obtain database connections.
serverName	string	localhost	Server where the database is running.
serviceName	string		JDBC driver property: serviceName.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**jobStore > dataSource > properties.sybase**

Data source properties for Sybase JDBC driver.

false

Attribute name	Data type	Default value	Description
SERVER_INITIATED_TRANSACTIONS	<ul style="list-style-type: none"> <li>false</li> <li>true</li> </ul>	false	JDBC driver property: SERVER_INITIATED_TRANSACTIONS.  <b>false</b> false <b>true</b> true
connectionProperties	string	SELECT_OPENS_CURSOR=true	JDBC driver property: connectionProperties.
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	<ul style="list-style-type: none"> <li>• SSL</li> <li>• socket</li> </ul>		JDBC driver property: networkProtocol.  <b>SSL</b> SSL <b>socket</b> socket
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	5000	Port on which to obtain database connections.
resourceManagerName	string		JDBC driver property: resourceManagerName.
serverName	string	localhost	Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
version	int		JDBC driver property: version.

**jobStore > dataSource > recoveryAuthData**

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## BELL (bell)

This feature enables the configuration of Basic Extensions using Liberty Libraries (BELL). A BELL enables the server runtime to be extended using shared libraries.

- library
  - file
  - fileset
  - folder
- service

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
libraryRef	A reference to top level library element (string).		The library to use for the BELL.

### library

The library to use for the BELL.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

### library > file

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

### library > fileset

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

### library > folder

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

### service

The name of the service that the system will look up in the /META-INF/services folder. If not specified, the system discovers all services located in the META-INF/services folder.

false

string

## OSGi Applications Bundle Repository (bundleRepository)

An internal bundle repository, in which you can store the bundles for your OSGi applications.

- fileset

Attribute name	Data type	Default value	Description
filesetRef	List of references to top level fileset elements (comma-separated string).		Space separated list of fileset references
id	string		A unique configuration ID.
location	A file, directory or url.		Location of the remote repository expressed as an absolute URL or one relative to the server home directory.

### fileset

Space separated list of fileset references

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

## Contexts And Dependency Injection (CDI) V1.2 (cdi12)

Defines the behavior of the Contexts and Dependency Injection (CDI) v1.2.

Attribute name	Data type	Default value	Description
enableImplicitBeanArchives	boolean	true	The implicit bean archives are scanned for any bean discoveries.

## CDI Container (cdiContainer)

Defines behavior for the Contexts and Dependency Injection (CDI) container.

## Channel Framework (channelfw)

Defines channel and chain management settings.

Attribute name	Data type	Default value	Description
chainQuiesceTimeout	A period of time with millisecond precision	30s	Default amount of time to wait while quiescing chains. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
chainStartRetryAttempts	int Minimum: 0	60	Number of retry attempts to make per chain.

Attribute name	Data type	Default value	Description
chainStartRetryInterval	A period of time with millisecond precision	5s	Time interval between start retries. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
warningWaitTime	A period of time with millisecond precision	10s	Amount of time to wait before notifying of a missing factory configuration. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

## Classloading (classloading)

Global classloading

Attribute name	Data type	Default value	Description
useJarUrls	boolean	false	Whether to use jar: or wsjar: URLs for referencing files in archives

## Cloudant Builder (cloudant)

Configuration for a Cloudant Builder. A Cloudant Builder creates Cloudant Client instances, which can connect to a Cloudant Database.

- containerAuthData
- library
  - file
  - fileset
  - folder
- ssl

Attribute name	Data type	Default value	Description
account	string		Account name used to connect to a Cloudant database.

Attribute name	Data type	Default value	Description
connectTimeout	A period of time with millisecond precision	5m	The timeout to establish a connection. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.
disableSSLAuthentication	boolean	false	Disables host name verification and certificate chain validation.
id	string		A unique configuration ID.
jndiName	string		JNDI name.
libraryRef	A reference to top level library element (string).		Specifies a library that contains the Cloudant Client library and its dependencies.
maxConnections	int Minimum: 0	6	The maximum number of concurrent connections that a Cloudant Client can make to the host.
password	Reversably encoded password (string)		Password corresponding to your Cloudant user ID.
proxyPassword	Reversably encoded password (string)		Password corresponding to the user name for a proxy server to use when connecting to a Cloudant server.
proxyUrl	string		The URL of a proxy server to use when connecting to a Cloudant server.
proxyUser	string		User name for a proxy server to use when connecting to a Cloudant server.

Attribute name	Data type	Default value	Description
readTimeout	A period of time with millisecond precision	30s	Timeout value to wait for a response from an established client connection. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
sslRef	A reference to top level ssl element (string).		Specifies the SSL configuration that is needed to establish a secure connection.
url	string		URL for the Cloudant server, which includes the host and port.
username	string		The Cloudant user ID used to log in and access your databases.

#### containerAuthData

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

#### library

Specifies a library that contains the Cloudant Client library and its dependencies.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

### library > file

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

### library > fileset

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

### library > folder

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

### ssl

Specifies the SSL configuration that is needed to establish a secure connection.

false

Attribute name	Data type	Default value	Description
clientAuthentication	boolean	false	Specifies whether client authentication is enabled. If set to true then client authentication is required and the client must provide a certificate for the server trusts.
clientAuthenticationSupported	boolean	false	Specifies whether a client authentication is supported. If set to true then the client authentication support means the server will check trust from a client if the client presents a certificate.

Attribute name	Data type	Default value	Description
clientKeyAlias	string		Specifies the alias of the certificate in the keystore that is used as the key to send to a server that has client authentication enabled. This attribute is only needed if the keystore has more than one key entry.
enabledCiphers	string		Specifies a custom list of ciphers. Separate each cipher in the list with a space. The supported cipher will depend on the underlying JRE used. Please check the JRE for valid ciphers.
keyStoreRef	A reference to top level keyStore element (string).		A keystore containing key entries for the SSL repertoire. This attribute is required.
securityLevel	<ul style="list-style-type: none"> <li>• MEDIUM</li> <li>• CUSTOM</li> <li>• HIGH</li> <li>• LOW</li> </ul>	HIGH	<p>Specifies the cipher suite group used by the SSL handshake. HIGH are 3DES and 128 bit and higher ciphers, MEDIUM are DES and 40 bit ciphers, LOW are ciphers without encryption. If the enabledCiphers attribute is used the securityLevel list is ignored.</p> <p><b>MEDIUM</b> %repertoire.MEDIUM</p> <p><b>CUSTOM</b> %repertoire.CUSTOM</p> <p><b>HIGH</b> Cipher suites 3DES and 128 bit and higher</p> <p><b>LOW</b> %repertoire.LOW</p>
serverKeyAlias	string		Specifies the alias of the certificate in the keystore used as the server's key. This attribute is only needed if the keystore has more then one key entry.

Attribute name	Data type	Default value	Description
sslProtocol	string		The SSL handshake protocol. Protocol values can be found in the documentation for the underlying JRE's Java Secure Socket Extension (JSSE) provider. When using the IBM JRE the default value is SSL_TLS and when using the Oracle JRE the default value is SSL.
trustStoreRef	A reference to top level keyStore element (string).	\${keyStoreRef}	A keystore containing trusted certificate entries used by the SSL repertoire for signing verification. This attribute is optional. If unspecified, the same keystore is used for both key and trusted certificate entries.

## Cloudant Database (cloudantDatabase)

Configuration for a Cloudant Database.

- cloudant
  - containerAuthData
  - library
    - file
    - fileset
    - folder
  - ssl

Attribute name	Data type	Default value	Description
cloudantRef	A reference to top level cloudant element (string).		Specifies the builder for the Cloudant Client that will be used when connecting to this database.
create	boolean	true	Indicates that the Cloudant Client should create the database if it does not already exist.
databaseName	string		Name of the database.
id	string		A unique configuration ID.
jndiName	string		JNDI name.

### cloudant

Specifies the builder for the Cloudant Client that will be used when connecting to this database.

false

Attribute name	Data type	Default value	Description
account	string		Account name used to connect to a Cloudbant database.
connectTimeout	A period of time with millisecond precision	5m	The timeout to establish a connection. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.
disableSSLAuthentication	boolean	false	Disables host name verification and certificate chain validation.
jndiName	string		JNDI name.
libraryRef	A reference to top level library element (string).		Specifies a library that contains the Cloudbant Client library and its dependencies.
maxConnections	int Minimum: 0	6	The maximum number of concurrent connections that a Cloudbant Client can make to the host.
password	Reversably encoded password (string)		Password corresponding to your Cloudbant user ID.
proxyPassword	Reversably encoded password (string)		Password corresponding to the user name for a proxy server to use when connecting to a Cloudbant server.
proxyUrl	string		The URL of a proxy server to use when connecting to a Cloudbant server.
proxyUser	string		User name for a proxy server to use when connecting to a Cloudbant server.

Attribute name	Data type	Default value	Description
readTimeout	A period of time with millisecond precision	30s	Timeout value to wait for a response from an established client connection. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
sslRef	A reference to top level ssl element (string).		Specifies the SSL configuration that is needed to establish a secure connection.
url	string		URL for the Cloudant server, which includes the host and port.
username	string		The Cloudant user ID used to log in and access your databases.

#### **cloudant > containerAuthData**

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

#### **cloudant > library**

Specifies a library that contains the Cloudant Client library and its dependencies.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

**cloudant > library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**cloudant > library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**cloudant > library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**cloudant > ssl**

Specifies the SSL configuration that is needed to establish a secure connection.

false

Attribute name	Data type	Default value	Description
clientAuthentication	boolean	false	Specifies whether client authentication is enabled. If set to true then client authentication is required and the client must provide a certificate for the server trusts.
clientAuthenticationSupported	boolean	false	Specifies whether a client authentication is supported. If set to true then the client authentication support means the server will check trust from a client if the client presents a certificate.

Attribute name	Data type	Default value	Description
clientKeyAlias	string		Specifies the alias of the certificate in the keystore that is used as the key to send to a server that has client authentication enabled. This attribute is only needed if the keystore has more than one key entry.
enabledCiphers	string		Specifies a custom list of ciphers. Separate each cipher in the list with a space. The supported cipher will depend on the underlying JRE used. Please check the JRE for valid ciphers.
keyStoreRef	A reference to top level keyStore element (string).		A keystore containing key entries for the SSL repertoire. This attribute is required.
securityLevel	<ul style="list-style-type: none"> <li>• MEDIUM</li> <li>• CUSTOM</li> <li>• HIGH</li> <li>• LOW</li> </ul>	HIGH	<p>Specifies the cipher suite group used by the SSL handshake. HIGH are 3DES and 128 bit and higher ciphers, MEDIUM are DES and 40 bit ciphers, LOW are ciphers without encryption. If the enabledCiphers attribute is used the securityLevel list is ignored.</p> <p><b>MEDIUM</b> %repertoire.MEDIUM</p> <p><b>CUSTOM</b> %repertoire.CUSTOM</p> <p><b>HIGH</b> Cipher suites 3DES and 128 bit and higher</p> <p><b>LOW</b> %repertoire.LOW</p>
serverKeyAlias	string		Specifies the alias of the certificate in the keystore used as the server's key. This attribute is only needed if the keystore has more then one key entry.

Attribute name	Data type	Default value	Description
sslProtocol	string		The SSL handshake protocol. Protocol values can be found in the documentation for the underlying JRE's Java Secure Socket Extension (JSSE) provider. When using the IBM JRE the default value is SSL_TLS and when using the Oracle JRE the default value is SSL.
trustStoreRef	A reference to top level keyStore element (string).	\${keyStoreRef}	A keystore containing trusted certificate entries used by the SSL repertoire for signing verification. This attribute is optional. If unspecified, the same keystore is used for both key and trusted certificate entries.

## Cluster Member (clusterMember)

Static cluster member configuration.

Attribute name	Data type	Default value	Description
name	string	defaultCluster	The name of the static cluster this server belongs to.

## WebSphere Cluster Manager (clusterPluginConfig)

The Cluster Manager MBean configuration.

Attribute name	Data type	Default value	Description
outputDir	string	\${server.output.dir}/pluginConfig	The output directory of the merged plugin-cfg.xml files.

## Certificate Authority Signed Certificate (collectiveCertificate)

Certificate authority signed certificate for collective.

Attribute name	Data type	Default value	Description
rdn	string	DC=com.ibm.ws.collective	Configure expected RDN attribute for incoming collective certificate.

## Collective Controller (collectiveController)

### Collective controller replica configuration

Attribute name	Data type	Default value	Description
isInitialReplicaSet	boolean	true	A boolean value that specifies whether a collective controller replica is joining an existing replica set or defining a new one. By default, the initial replica set contains only the first collective controller replica. Specify a value of true in each replica in the initial replica set. Specify a value of false in each replica subsequently added to the initial replica set. If the replicaSet value is changed after it was initially defined, specify a value of false.
password	Reversably encoded password (string)		The password of the controller user
replicaHost	string	localhost	The host name or IP address associated with this collective controller's replication port.
replicaPort	int Minimum: 1 Maximum: 65535	10010	The port number assigned for this collective controller's replication port.
replicaSet	string	\${replicaHost}:\${replicaPort}	A space delimited list of collective controller replica endpoints. The set of endpoints is used by this replica to establish contact with other replicas in the set. The list does not need to contain all replicas, but must contain at least one replica from the initial replica set. An endpoint is defined as a host:port pair, for example localhost:10010
repositoryDir	string	\${server.output.dir}/resources/collective/repository	The path on the local file system within which the replica's repository contents should be stored. The directory should have the necessary permissions to enable the process to read, write, and create files.
user	string		The user ID of the controller

## Collective Member (collectiveMember)

The collective member configuration requires at least one collective controller address (identified by controllerHost and controllerPort). The collective controller can have multiple available addresses. Add one or more failoverController elements to identify the additional controllers. When multiple controllers are available, the member connects to one of the controllers. If the connection to the controller ends unexpectedly, the member connects to another controller in the remaining set of controllers.

- failoverController

Attribute name	Data type	Default value	Description
controllerHost	string		The host name for the collective controller instance.
controllerPort	int		The port for the JMX/REST connector, typically the HTTPS port.
controllerReadTimeout	A period of time with millisecond precision	300s	The read timeout for member connection to the collective controller. A longer read timeout may be necessary in large or geographically dispersed topologies. Minimum value is 2 minutes. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
heartBeatInterval	A period of time with millisecond precision	60s	Periodic time interval at which the collective member will contact the collective controller to indicate liveness. Minimum value is 1 second. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

### failoverController

An additional collective controller address which is available for the collective member to use.

false

Attribute name	Data type	Default value	Description
host	string		The host name for the collective controller instance.
id	string		A unique configuration ID.
port	int		The port for the JMX/REST connector, typically the HTTPS port.

## WebSphere Collective Repository MBean (collectiveRepository)

The Collective Repository MBean configuration.

Attribute name	Data type	Default value	Description
maxMemberConnections	int	2147483647	The maximum number of members permitted to connect to the repository.

## Configuration Management (config)

Defines how the server processes configuration information.

Attribute name	Data type	Default value	Description
monitorInterval	A period of time with millisecond precision	500ms	Rate at which the server checks for configuration updates. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Action to take after a incurring a configuration error.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

Attribute name	Data type	Default value	Description
updateTrigger	<ul style="list-style-type: none"> <li>mbean</li> <li>polled</li> <li>disabled</li> </ul>	polled	<p>Configuration update method or trigger.</p> <p><b>mbean</b> Server will only update the configuration when prompted by the FileNotificationMbean. The FileNotificationMbean is typically called by an external program such as an integrated development environment or a management application.</p> <p><b>polled</b> Server will scan for changes at the polling interval on all the configuration files and update the runtime configuration with the changes detected.</p> <p><b>disabled</b> Disables all update monitoring. Configuration changes will not be applied while the server is running.</p>

## Connection Factory (connectionFactory)

Defines a connection factory configuration.

- connectionManager
- containerAuthData
- recoveryAuthData

Attribute name	Data type	Default value	Description
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a connection factory.

Attribute name	Data type	Default value	Description
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.
id	string		A unique configuration ID.
jndiName	string		JNDI name for a resource.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.

### connectionManager

Connection manager for a connection factory.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.

Attribute name	Data type	Default value	Description
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.

Attribute name	Data type	Default value	Description
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

#### containerAuthData

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

### recoveryAuthData

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## Connection Manager (connectionManager)

Connection Manager configuration

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
id	string		A unique configuration ID.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.

Attribute name	Data type	Default value	Description
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

## Thread Context Propagation (contextService)

Configures how context is propagated to threads

- baseContext
  - baseContext
  - classloaderContext
  - jeeMetadataContext
  - securityContext
  - syncToOSThreadContext
  - zosWLMContext

- classloaderContext
- jeeMetadataContext
- securityContext
- syncToOSThreadContext
- zosWLMContext

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
id	string		A unique configuration ID.
jndiName	string		JNDI name
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

### baseContext

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
id	string		A unique configuration ID.
jndiName	string		JNDI name
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**baseContext > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

com.ibm.ws.context.service-factory

**baseContext > classloaderContext**

Classloader context propagation configuration.

false

**baseContext > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**baseContext > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**baseContext > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**baseContext > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"><li>• Propagate</li><li>• PropagateOrNew</li><li>• New</li></ul>	Propagate	Indicates how the WLM context should be handled for non-Daemon work.  <b>Propagate</b> Use the same WLM Context (if one exists).  <b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists.  <b>New</b> Always create a new WLM context.

**classloaderContext**

Classloader context propagation configuration.

false

**jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

### syncToOSThreadContext

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

### zosWLMContext

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"><li>• Propagate</li><li>• PropagateOrNew</li><li>• New</li></ul>	Propagate	Indicates how the WLM context should be handled for non-Daemon work. <b>Propagate</b> Use the same WLM Context (if one exists). <b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists. <b>New</b> Always create a new WLM context.

## Cross-Origin Resource Sharing (cors)

Refers to a cross-domain security procedure for JavaScript-based clients.

Attribute name	Data type	Default value	Description
allowCredentials	boolean		A boolean that indicates if the user credentials can be included in the request.
allowedHeaders	string		A comma-separated list of HTTP headers allowed to be used by the origin domain when making requests to the configured domain.

Attribute name	Data type	Default value	Description
allowedMethods	string		A comma-separated list of HTTP methods allowed to be used by the origin domain when making requests to the configured domain.
allowedOrigins	string	null	A comma-separated list of origins allowed to access the configured domain.
domain	string		The domain name represents the URL being setup with these CORS settings.
exposeHeaders	string		A comma-separated list of HTTP headers that are safe to expose to the calling API.
id	string		A unique configuration ID.
maxAge	long		A long that indicates how many seconds a response to a preflight request can be cached in the browser.

## CouchDB (couchdb)

Configuration for a CouchDB Connector.

- library
  - file
  - fileset
  - folder

Attribute name	Data type	Default value	Description
caching	boolean	true	Allows loading documents from http client's cache if it exists and the revision has not changed since last access.
cleanupIdleConnections	boolean	true	Closes connections automatically when they are considered idle.
connectionTimeout	A period of time with millisecond precision	30s	The timeout to establish a connection. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
enableSSL	boolean	false	Enables SSL when connecting to CouchDB.
host	string		Host name for the CouchDB server.
id	string		A unique configuration ID.
jndiName	string		JNDI name for a CouchDB instance.
libraryRef	A reference to top level library element (string).		Specifies a library that contains the CouchDB Client library and its dependencies.
maxCacheEntries	int Minimum: 0	1000	The maximum number of cache entries for the http client.
maxConnections	int	20	The maximum number of concurrent connections to the host.
maxObjectSizeBytes	int Minimum: 0	8192	Sets the maximum size for a stored document.
password	Reversably encoded password (string)		Password corresponding to your Couchdb User ID.
port	int	5984	Port number for the CouchDB server.
relaxedSSLSettings	boolean	false	Enables relaxed SSL settings which allows the trust manager to accept any host and certificate.
socketTimeout	A period of time with millisecond precision	1m	The duration to wait for a response. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
url	string		URL for the CouchDB server, which includes the host and port.
useExpectContinue	boolean	true	Use Expect Continue header in request when making requests to CouchDB.
username	string		The CouchDB User ID used to log-in and access your DBs.

## library

Specifies a library that contains the CouchDB Client library and its dependencies.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

### library > file

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

### library > fileset

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

### library > folder

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

## Custom LDAP Filters (customLdapFilterProperties)

Specifies the list of default Custom LDAP filters.

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(!(objectclass=groupOfNames)(!(objectclass=groupOfUniqueNames)(objectclass=groupOfUniqueNames)))	An LDAP filter clause for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	ibm-allGroups:member;ibm-allGroups:uniqueMember;groupOfNames:member;groupOfUniqueNames:member	An LDAP filter that maps group memberships.
id	string		A unique configuration ID.
userFilter	string	(&(uid=%v)(objectclass=ePerson))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	*:uid	An LDAP filter that maps the name of a user to an LDAP entry.

## Data Source (dataSource)

Defines a data source configuration.

- connectionManager
- containerAuthData
- jaasLoginContextEntry
- jdbcDriver
  - library
    - file
    - fileset
    - folder
- properties
- properties.datadirect.sqlserver
- properties.db2.i.native
- properties.db2.i.toolbox
- properties.db2.jcc
- properties.derby.client
- properties.derby.embedded
- properties.informix
- properties.informix.jcc
- properties.microsoft.sqlserver
- properties.oracle
- properties.sybase
- recoveryAuthData

Attribute name	Data type	Default value	Description
beginTranForResultSetScrolling	boolean	true	Attempt transaction enlistment when result set scrolling interfaces are used.
beginTranForVendorAPIs	boolean	true	Attempt transaction enlistment when vendor interfaces are used.
commitOrRollbackOnCleanup	<ul style="list-style-type: none"> <li>• commit</li> <li>• rollback</li> </ul>		<p>Determines how to clean up connections that might be in a database unit of work (AutoCommit=false) when the connection is closed or returned to the pool.</p> <p><b>commit</b> Clean up the connection by committing.</p> <p><b>rollback</b> Clean up the connection by rolling back.</p>

Attribute name	Data type	Default value	Description
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a data source.
connectionSharing	<ul style="list-style-type: none"> <li>MatchOriginalRequest</li> <li>MatchCurrentState</li> </ul>	MatchOriginalRequest	<p>Specifies how connections are matched for sharing.</p> <p><b>MatchOriginalRequest</b> When sharing connections, match based on the original connection request.</p> <p><b>MatchCurrentState</b> When sharing connections, match based on the current state of the connection.</p>
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.
enableConnectionCasting	boolean	false	Indicates that connections obtained from the data source should be castable to interface classes that the JDBC vendor connection implementation implements. Enabling this option incurs additional overhead on each getConnection operation. If vendor JDBC interfaces are needed less frequently, it might be more efficient to leave this option disabled and use Connection.unwrap(interface) only where it is needed.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
isolationLevel	<ul style="list-style-type: none"> <li>• TRANSACTION_REPEATABLE_READ</li> <li>• TRANSACTION_READ_COMMITTED</li> <li>• TRANSACTION_SERIALIZABLE</li> <li>• TRANSACTION_READ_UNCOMMITTED</li> <li>• TRANSACTION_SNAPSHOT</li> </ul>		<p>Default transaction isolation level.</p> <p><b>TRANSACTION_REPEATABLE_READ</b> Dirty reads and non-repeatable reads are prevented; phantom reads can occur.</p> <p><b>TRANSACTION_READ_COMMITTED</b> Dirty reads are prevented; non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SERIALIZABLE</b> Dirty reads, non-repeatable reads and phantom reads are prevented.</p> <p><b>TRANSACTION_READ_UNCOMMITTED</b> Dirty reads, non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SNAPSHOT</b> Snapshot isolation for Microsoft SQL Server JDBC Driver and DataDirect Connect for JDBC driver.</p>
jaasLoginContextEntryRef	A reference to top level jaasLoginContextEntry element (string).		JAAS login context entry for authentication.
jdbcDriverRef	A reference to top level jdbcDriver element (string).		JDBC driver for a data source.
jndiName	string		JNDI name for a data source.

Attribute name	Data type	Default value	Description
queryTimeout	A period of time with second precision		Default query timeout for SQL statements. In a JTA transaction, syncQueryTimeoutWithTransactionTimeout can override this default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.
statementCacheSize	int Minimum: 0	10	Maximum number of cached statements per connection.
supplementalJDBCTrace	boolean		Supplements the JDBC driver trace that is logged when JDBC driver trace is enabled in bootstrap.properties. JDBC driver trace specifications include: com.ibm.ws.database.logwriter, com.ibm.ws.db2.logwriter, com.ibm.ws.derby.logwriter, com.ibm.ws.informix.logwriter, com.ibm.ws.oracle.logwriter, com.ibm.ws.sqlserver.logwriter, com.ibm.ws.sybase.logwriter
syncQueryTimeoutWithTransactionTimeout	boolean	false	Use the time remaining (if any) in a JTA transaction as the default query timeout for SQL statements.
transactional	boolean	true	Enable participation in transactions that are managed by the application server.
type	<ul style="list-style-type: none"> <li>javax.sql.DataSource</li> <li>javax.sql.XADataSource</li> <li>javax.sql.ConnectionPoolDataSource</li> </ul>		Type of data source. <b>javax.sql.DataSource</b> javax.sql.DataSource <b>javax.sql.XADataSource</b> javax.sql.XADataSource <b>javax.sql.ConnectionPoolDataSource</b> javax.sql.ConnectionPoolDataSource

### connectionManager

Connection manager for a data source.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.

Attribute name	Data type	Default value	Description
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**containerAuthData**

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

### jaasLoginContextEntry

JAAS login context entry for authentication.

false

Attribute name	Data type	Default value	Description
loginModuleRef	List of references to top level jaasLoginModule elements (comma-separated string).	hashtable,userNameAndPassword,certificate,clientId	Word, certificate, clientId of a JAAS login module.
name	string		Name of a JAAS configuration entry.

### jdbcDriver

JDBC driver for a data source.

false

Attribute name	Data type	Default value	Description
javax.sql.ConnectionPoolDataSource	string		JDBC driver implementation of javax.sql.ConnectionPoolDataSource.
javax.sql.DataSource	string		JDBC driver implementation of javax.sql.DataSource.
javax.sql.XADataSource	string		JDBC driver implementation of javax.sql.XADataSource.
libraryRef	A reference to top level library element (string).		Identifies JDBC driver JARs and native files.

### jdbcDriver > library

Identifies JDBC driver JARs and native files.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

**jdbcDriver > library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**jdbcDriver > library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**jdbcDriver > library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**properties**

List of JDBC vendor properties for the data source. For example, `databaseName="dbname"`  
`serverName="localhost"` `portNumber="50000"`.

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database.
databaseName	string		JDBC driver property: databaseName.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
serverName	string		Server where the database is running.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

### properties.datadirect.sqlserver

Data source properties for the DataDirect Connect for JDBC driver for Microsoft SQL Server.

false

Attribute name	Data type	Default value	Description
JDBCBehavior	<ul style="list-style-type: none"> <li>• 1</li> <li>• 0</li> </ul>	0	JDBC driver property: JDBCBehavior. Values are: 0 (JDBC 4.0) or 1 (JDBC 3.0).  <b>1</b> JDBC 3.0 <b>0</b> JDBC 4.0
XATransactionGroup	string		JDBC driver property: XATransactionGroup.
XMLDescribeType	<ul style="list-style-type: none"> <li>• longvarbinary</li> <li>• longvarchar</li> </ul>		JDBC driver property: XMLDescribeType.  <b>longvarbinary</b> longvarbinary  <b>longvarchar</b> longvarchar
accountingInfo	string		JDBC driver property: accountingInfo.
alternateServers	string		JDBC driver property: alternateServers.
alwaysReportTriggerResults	boolean		JDBC driver property: alwaysReportTriggerResults.
applicationName	string		JDBC driver property: applicationName.
authenticationMethod	<ul style="list-style-type: none"> <li>• ntlm</li> <li>• userIdPassword</li> <li>• kerberos</li> <li>• auto</li> </ul>		JDBC driver property: authenticationMethod.  <b>ntlm</b> ntlm <b>userIdPassword</b> userIdPassword  <b>kerberos</b> kerberos  <b>auto</b> auto
bulkLoadBatchSize	long		JDBC driver property: bulkLoadBatchSize.
bulkLoadOptions	long		JDBC driver property: bulkLoadOptions.
clientHostName	string		JDBC driver property: clientHostName.
clientUser	string		JDBC driver property: clientUser.

Attribute name	Data type	Default value	Description
codePageOverride	string		JDBC driver property: codePageOverride.
connectionRetryCount	int		JDBC driver property: connectionRetryCount.
connectionRetryDelay	A period of time with second precision		JDBC driver property: connectionRetryDelay. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
convertNull	int		JDBC driver property: convertNull.
databaseName	string		JDBC driver property: databaseName.
dateTimeInputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeInputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
dateTimeOutputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeOutputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
describeInputParameters	<ul style="list-style-type: none"> <li>• describeIfString</li> <li>• noDescribe</li> <li>• describeIfDateTime</li> <li>• describeAll</li> </ul>		JDBC driver property: describeInputParameters.  <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll

Attribute name	Data type	Default value	Description
describeOutputParameters	<ul style="list-style-type: none"> <li>describeIfString</li> <li>noDescribe</li> <li>describeIfDateTime</li> <li>describeAll</li> </ul>		JDBC driver property: describeOutputParameters. <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll
enableBulkLoad	boolean		JDBC driver property: enableBulkLoad.
enableCancelTimeout	boolean		JDBC driver property: enableCancelTimeout.
encryptionMethod	<ul style="list-style-type: none"> <li>loginSSL</li> <li>requestSSL</li> <li>SSL</li> <li>noEncryption</li> </ul>		JDBC driver property: encryptionMethod. <b>loginSSL</b> loginSSL <b>requestSSL</b> requestSSL <b>SSL</b> SSL <b>noEncryption</b> noEncryption
failoverGranularity	<ul style="list-style-type: none"> <li>disableIntegrityCheck</li> <li>atomicWithRepositioning</li> <li>nonAtomic</li> <li>atomic</li> </ul>		JDBC driver property: failoverGranularity. <b>disableIntegrityCheck</b> disableIntegrityCheck <b>atomicWithRepositioning</b> atomicWithRepositioning <b>nonAtomic</b> nonAtomic <b>atomic</b> atomic
failoverMode	<ul style="list-style-type: none"> <li>connect</li> <li>select</li> <li>extended</li> </ul>		JDBC driver property: failoverMode. <b>connect</b> connect <b>select</b> select <b>extended</b> extended
failoverPreconnect	boolean		JDBC driver property: failoverPreconnect.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
initializationString	string		JDBC driver property: initializationString.
insensitiveResultSetBufferSize	int		JDBC driver property: insensitiveResultSetBufferSize.

Attribute name	Data type	Default value	Description
javaDoubleToString	boolean		JDBC driver property: javaDoubleToString.
loadBalancing	boolean		JDBC driver property: loadBalancing.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
longDataCacheSize	int Minimum: -1		JDBC driver property: longDataCacheSize.
netAddress	string		JDBC driver property: netAddress.
packetSize	int Minimum: -1 Maximum: 128		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
queryTimeout	A period of time with second precision		JDBC driver property: queryTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
resultsetMetaDataOptions	int		JDBC driver property: resultSetMetaDataOptions.
selectMethod	<ul style="list-style-type: none"> <li>• direct</li> <li>• cursor</li> </ul>		JDBC driver property: selectMethod.  <b>direct</b> direct <b>cursor</b> cursor
serverName	string	localhost	Server where the database is running.
snapshotSerializable	boolean		JDBC driver property: snapshotSerializable.

Attribute name	Data type	Default value	Description
spyAttributes	string		JDBC driver property: spyAttributes.
stringInputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringInputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
stringOutputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringOutputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
suppressConnectionWarnings	boolean		JDBC driver property: suppressConnectionWarnings.
transactionMode	<ul style="list-style-type: none"> <li>explicit</li> <li>implicit</li> </ul>		JDBC driver property: transactionMode. <b>explicit</b> explicit <b>implicit</b> implicit
truncateFractionalSeconds	boolean		JDBC driver property: truncateFractionalSeconds.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
useServerSideUpdatableCursors	boolean		JDBC driver property: useServerSideUpdatableCursors.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
validateServerCertificate	boolean		JDBC driver property: validateServerCertificate.

### properties.db2.i.native

Data source properties for the IBM DB2 for i Native JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>read only</li> <li>all</li> <li>read call</li> </ul>	all	JDBC driver property: access. <b>read only</b> read only <b>all</b> all <b>read call</b> read call

Attribute name	Data type	Default value	Description
autoCommit	boolean	true	JDBC driver property: autoCommit.
batchStyle	<ul style="list-style-type: none"> <li>• 2.1</li> <li>• 2.0</li> </ul>	2.0	JDBC driver property: batchStyle. <b>2.1</b> 2.1 <b>2.0</b> 2.0
behaviorOverride	int		JDBC driver property: behaviorOverride.
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive
dataTruncation	string	true	JDBC driver property: dataTruncation.
databaseName	string	*LOCAL	JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy
dateSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		JDBC driver property: dateSeparator. <b>\,</b> The comma character (,). <b>b</b> The character b <b>.</b> The period character (.). <b>/</b> The forward slash character (/). <b>-</b> The dash character (-).
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		JDBC driver property: decimalSeparator. <b>\,</b> The comma character (,). <b>.</b> The period character (.).
directMap	boolean	true	JDBC driver property: directMap.
doEscapeProcessing	boolean	true	JDBC driver property: doEscapeProcessing.
fullErrors	boolean		JDBC driver property: fullErrors.
libraries	string		JDBC driver property: libraries.
lobThreshold	int Maximum: 500000	0	JDBC driver property: lobThreshold.

Attribute name	Data type	Default value	Description
lockTimeout	A period of time with second precision	0	JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>• 31</li> <li>• 63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 63
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
networkProtocol	int		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
prefetch	boolean	true	JDBC driver property: prefetch.
queryOptimizeGoal	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>	2	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).  <b>2</b> *ALLIO <b>1</b> *FIRSTIO

Attribute name	Data type	Default value	Description
reuseObjects	boolean	true	JDBC driver property: reuseObjects.
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
systemNaming	boolean	false	JDBC driver property: systemNaming.
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat.  <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  \,    The comma character (,). <b>b</b> The character b :    The colon character (:). .    The period character (.).
trace	boolean		JDBC driver property: trace.
transactionTimeout	A period of time with second precision	0	JDBC driver property: transactionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateHex	<ul style="list-style-type: none"> <li>• binary</li> <li>• character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
useBlockInsert	boolean	false	JDBC driver property: useBlockInsert.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

### properties.db2.i.toolbox

Data source properties for the IBM DB2 for i Toolbox JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>• read only</li> <li>• all</li> <li>• read call</li> </ul>	all	JDBC driver property: access. <b>read only</b> read only <b>all</b> all <b>read call</b> read call
behaviorOverride	int		JDBC driver property: behaviorOverride.
bidImplicitReordering	boolean	true	JDBC driver property: bidImplicitReordering.
bidNumericOrdering	boolean	false	JDBC driver property: bidNumericOrdering.
bidStringType	int		JDBC driver property: bidStringType.
bigDecimal	boolean	true	JDBC driver property: bigDecimal.
blockCriteria	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>	2	JDBC driver property: blockCriteria. Values are: 0 (no record blocking), 1 (block if FOR FETCH ONLY is specified), 2 (block if FOR UPDATE is specified). <b>2</b> 2 <b>1</b> 1 <b>0</b> 0

Attribute name	Data type	Default value	Description
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> <li>• insensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive <b>insensitive</b> insensitive
dataCompression	boolean	true	JDBC driver property: dataCompression.
dataTruncation	boolean	true	JDBC driver property: dataTruncation.
databaseName	string		JDBC driver property: databaseName.
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy

Attribute name	Data type	Default value	Description
dateSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		<p>JDBC driver property: dateSeparator.</p> <p>The space character ( ).</p> <p>\, The comma character (,).</p> <p>. The period character (.).</p> <p>/ The forward slash character (/).</p> <p>- The dash character (-).</p>
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		<p>JDBC driver property: decimalSeparator.</p> <p>\, The comma character (,).</p> <p>. The period character (.).</p>
driver	<ul style="list-style-type: none"> <li>• toolbox</li> <li>• native</li> </ul>	toolbox	<p>JDBC driver property: driver.</p> <p><b>toolbox</b> toolbox</p> <p><b>native</b> native</p>
errors	<ul style="list-style-type: none"> <li>• full</li> <li>• basic</li> </ul>	basic	<p>JDBC driver property: errors.</p> <p><b>full</b> full</p> <p><b>basic</b> basic</p>
extendedDynamic	boolean	false	JDBC driver property: extendedDynamic.
extendedMetaData	boolean	false	JDBC driver property: extendedMetaData.
fullOpen	boolean	false	JDBC driver property: fullOpen.
holdInputLocators	boolean	true	JDBC driver property: holdInputLocators.
holdStatements	boolean	false	JDBC driver property: holdStatements.
isolationLevelSwitchingSupport	boolean	false	JDBC driver property: isolationLevelSwitchingSupport.
keepAlive	boolean		JDBC driver property: keepAlive.
lazyClose	boolean	false	JDBC driver property: lazyClose.
libraries	string		JDBC driver property: libraries.

Attribute name	Data type	Default value	Description
lobThreshold	int Minimum: 0 Maximum: 16777216	0	JDBC driver property: lobThreshold.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>• 31</li> <li>• 63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 64
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
metaDataSource	int Minimum: 0 Maximum: 1	1	JDBC driver property: metaDataSource.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
naming	<ul style="list-style-type: none"> <li>• system</li> <li>• sql</li> </ul>	sql	JDBC driver property: naming.  <b>system</b> system <b>sql</b> sql
package	string		JDBC driver property: package.
packageAdd	boolean	true	JDBC driver property: packageAdd.
packageCCSID	<ul style="list-style-type: none"> <li>• 13488</li> <li>• 1200</li> </ul>	13488	JDBC driver property: packageCCSID. Values are: 1200 (UCS-2) or 13488 (UTF-16).  <b>13488</b> 13488 (UTF-16) <b>1200</b> 1200 (UCS-2)
packageCache	boolean	false	JDBC driver property: packageCache.

Attribute name	Data type	Default value	Description
packageCriteria	<ul style="list-style-type: none"> <li>default</li> <li>select</li> </ul>	default	JDBC driver property: packageCriteria. <b>default</b> default <b>select</b> select
packageError	<ul style="list-style-type: none"> <li>exception</li> <li>none</li> <li>warning</li> </ul>	warning	JDBC driver property: packageError. <b>exception</b> exception <b>none</b> none <b>warning</b> warning
packageLibrary	string	QGPL	JDBC driver property: packageLibrary.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
prefetch	boolean	true	JDBC driver property: prefetch.
prompt	boolean	false	JDBC driver property: prompt.
proxyServer	string		JDBC driver property: proxyServer.
qaqqiniLibrary	string		JDBC driver property: qaqqiniLibrary.
queryOptimizeGoal	int Minimum: 0 Maximum: 2	0	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).
receiveBufferSize	int Minimum: 1		JDBC driver property: receiveBufferSize.
remarks	<ul style="list-style-type: none"> <li>system</li> <li>sql</li> </ul>	system	JDBC driver property: remarks. <b>system</b> system <b>sql</b> sql
rollbackCursorHold	boolean	false	JDBC driver property: rollbackCursorHold.
savePasswordWhenSerialized	boolean	false	JDBC driver property: savePasswordWhenSerialized.
secondaryUrl	string		JDBC driver property: secondaryUrl.
secure	boolean	false	JDBC driver property: secure.
sendBufferSize	int Minimum: 1		JDBC driver property: sendBufferSize.

Attribute name	Data type	Default value	Description
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
soLinger	A period of time with second precision		JDBC driver property: soLinger. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
soTimeout	A period of time with millisecond precision		JDBC driver property: soTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
sort	<ul style="list-style-type: none"> <li>• hex</li> <li>• table</li> <li>• language</li> </ul>	hex	JDBC driver property: sort. <b>hex</b> hex <b>table</b> table <b>language</b> language
sortLanguage	string		JDBC driver property: sortLanguage.
sortTable	string		JDBC driver property: sortTable.
sortWeight	<ul style="list-style-type: none"> <li>• unqiue</li> <li>• shared</li> </ul>		JDBC driver property: sortWeight. <b>unqiue</b> unique <b>shared</b> shared
tcpNoDelay	boolean		JDBC driver property: tcpNoDelay.
threadUsed	boolean	true	JDBC driver property: threadUsed.

Attribute name	Data type	Default value	Description
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat. <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  The space character ( ). \, The comma character (,). : The colon character (:). . The period character (.).
toolboxTrace	<ul style="list-style-type: none"> <li>• diagnostic</li> <li>• information</li> <li>• conversion</li> <li>• error</li> <li>• thread</li> <li>• proxy</li> <li>• none</li> <li>• datastream</li> <li>• pcml</li> <li>• all</li> <li>• jdbc</li> <li>• warning</li> </ul>		JDBC driver property: toolboxTrace. <b>diagnostic</b> diagnostic <b>information</b> information <b>conversion</b> conversion <b>error</b> error <b>thread</b> thread <b>proxy</b> proxy <b>none</b> none <b>datastream</b> datastream <b>pcml</b> pcml <b>all</b> all <b>jdbc</b> jdbc <b>warning</b> warning
trace	boolean		JDBC driver property: trace.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateBoolean	boolean	true	JDBC driver property: translateBoolean.

Attribute name	Data type	Default value	Description
translateHex	<ul style="list-style-type: none"> <li>binary</li> <li>character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
trueAutoCommit	boolean	false	JDBC driver property: trueAutoCommit.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaLooselyCoupledSupport	int  Minimum: 0  Maximum: 1	0	JDBC driver property: xaLooselyCoupledSupport.

### properties.db2.jcc

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for DB2.

false

Attribute name	Data type	Default value	Description
activateDatabase	int		JDBC driver property: activateDatabase.
alternateGroupDatabaseName	string		JDBC driver property: alternateGroupDatabaseName.
alternateGroupPortNumber	string		JDBC driver property: alternateGroupPortNumber.
alternateGroupServerName	string		JDBC driver property: alternateGroupServerName.
blockingReadConnectionTimeout	A period of time with second precision		JDBC driver property: blockingReadConnectionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
clientAccountingInformation	string		JDBC driver property: clientAccountingInformation.
clientApplicationInformation	string		JDBC driver property: clientApplicationInformation.
clientRerouteAlternatePortNumber	string		JDBC driver property: clientRerouteAlternatePortNumber.
clientRerouteAlternateServerName	string		JDBC driver property: clientRerouteAlternateServerName.

Attribute name	Data type	Default value	Description
clientUser	string		JDBC driver property: clientUser.
clientWorkstation	string		JDBC driver property: clientWorkstation.
connectionCloseWithInFlightTransaction	Transaction • 1		JDBC driver property: connectionCloseWithInFlightTransaction. 2 CONNECTION_CLOSE_WITH_ROLLBACK 1 CONNECTION_CLOSE_WITH_EXCEPTION
currentAlternateGroupEntry	int		JDBC driver property: currentAlternateGroupEntry.
currentFunctionPath	string		JDBC driver property: currentFunctionPath.
currentLocaleLcCtype	string		JDBC driver property: currentLocaleLcCtype.
currentLockTimeout	A period of time with second precision		JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
currentPackagePath	string		JDBC driver property: currentPackagePath.
currentPackageSet	string		JDBC driver property: currentPackageSet.
currentSQLID	string		JDBC driver property: currentSQLID.
currentSchema	string		JDBC driver property: currentSchema.
cursorSensitivity	• 2 • 1 • 0		JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). 2 TYPE_SCROLL_ASENSITIVE 1 TYPE_SCROLL_SENSITIVE_DYNAMIC 0 TYPE_SCROLL_SENSITIVE_STATIC
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean	true	JDBC driver property: deferPrepares.

Attribute name	Data type	Default value	Description
driverType	<ul style="list-style-type: none"> <li>2</li> <li>4</li> </ul>	4	JDBC driver property: driverType. 2 Type 2 JDBC driver. 4 Type 4 JDBC driver.
enableAlternateGroupSeamlessACR	boolean		JDBC driver property: enableAlternateGroupSeamlessACR.
enableClientAffinitiesList	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableClientAffinitiesList. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableExtendedDescribe	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedDescribe. 2 NO 1 YES
enableExtendedIndicators	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedIndicators. 2 NO 1 YES
enableNamedParameterMarkers	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSeamlessFailover	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeInputStreams	boolean		JDBC driver property: fullyMaterializeInputStreams.
fullyMaterializeInputStreamsOnBatchExecution	<ul style="list-style-type: none"> <li>1</li> </ul>		JDBC driver property: fullyMaterializeInputStreamsOnBatchExecution. 2 NO 1 YES
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.

Attribute name	Data type	Default value	Description
implicitRollbackOption	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: implicitRollbackOption.</p> <p>2 IMPLICIT_ROLLBACK_OPTION_N 1 IMPLICIT_ROLLBACK_OPTION_N 0 IMPLICIT_ROLLBACK_OPTION_N</p>
interruptProcessingMode	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: interruptProcessingMode.</p> <p>2 INTERRUPT_PROCESSING_MODI 1 INTERRUPT_PROCESSING_MODI 0 INTERRUPT_PROCESSING_MODI</p>
keepAliveTimeOut	A period of time with second precision		<p>JDBC driver property: keepAliveTimeOut. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
keepDynamic	int		JDBC driver property: keepDynamic.
kerberosServerPrincipal	string		JDBC driver property: kerberosServerPrincipal.
loginTimeout	A period of time with second precision		<p>JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
maxConnCachedParamBufferSize	int		JDBC driver property: maxConnCachedParamBufferSize.
maxRetriesForClientReroute	int		JDBC driver property: maxRetriesForClientReroute.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	50000	Port on which to obtain database connections.
profileName	string		JDBC driver property: profileName.

Attribute name	Data type	Default value	Description
queryCloseImplicit	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: queryCloseImplicit. Values are: 1 (QUERY_CLOSE_IMPLICIT_YES) or 2 (QUERY_CLOSE_IMPLICIT_NO). 2 QUERY_CLOSE_IMPLICIT_NO 1 QUERY_CLOSE_IMPLICIT_YES
queryDataSize	int Minimum: 4096 Maximum: 65535		JDBC driver property: queryDataSize.
queryTimeoutInterruptProcessingMode	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: queryTimeoutInterruptProcessingMode. 2 INTERRUPT_PROCESSING_MODE_C 1 INTERRUPT_PROCESSING_MODE_S
readOnly	boolean		JDBC driver property: readOnly.
recordTemporalHistory	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: recordTemporalHistory. 2 NO 1 YES
resultSetHoldability	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT). 2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT). 2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT
retrieveMessagesFromServerOnGetMessage	boolean	true	JDBC driver property: retrieveMessagesFromServerOnGetMessage.

Attribute name	Data type	Default value	Description
retryIntervalForClientReroute	A period of time with second precision		JDBC driver property: retryIntervalForClientReroute. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 18</li> <li>• 15</li> <li>• 9</li> <li>• 16</li> <li>• 13</li> <li>• 11</li> <li>• 12</li> </ul>		<p>JDBC driver property: securityMechanism. Values are:</p> <ul style="list-style-type: none"> <li>3 (CLEAR_TEXT_PASSWORD_SECURITY),</li> <li>4 (USER_ONLY_SECURITY),</li> <li>7 (ENCRYPTED_PASSWORD_SECURITY),</li> <li>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY),</li> <li>11 (KERBEROS_SECURITY),</li> <li>12 (ENCRYPTED_USER_AND_DATA_SECURITY),</li> <li>13 (ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY),</li> <li>15 (PLUGIN_SECURITY),</li> <li>16 (ENCRYPTED_USER_ONLY_SECURITY),</li> <li>18 (TLS_CLIENT_CERTIFICATE_SECURITY).</li> </ul> <p>3 CLEAR_TEXT_PASSWORD_SECURITY</p> <p>7 ENCRYPTED_PASSWORD_SECURITY</p> <p>4 USER_ONLY_SECURITY</p> <p>18 TLS_CLIENT_CERTIFICATE_SECURITY</p> <p>15 PLUGIN_SECURITY</p> <p>9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p> <p>16 ENCRYPTED_USER_ONLY_SECURITY</p> <p>13 ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY</p> <p>11 KERBEROS_SECURITY</p> <p>12 ENCRYPTED_USER_AND_DATA_SECURITY</p>
sendDataAsIs	boolean		JDBC driver property: sendDataAsIs.
serverName	string	localhost	Server where the database is running.
sessionTimeZone	string		JDBC driver property: sessionTimeZone.
sqljCloseStmtsWithOpenResultSet	boolean		JDBC driver property: sqljCloseStmtsWithOpenResultSet.

Attribute name	Data type	Default value	Description
sqljEnableClassLoaderSpecificProfiles	boolean		JDBC driver property: sqljEnableClassLoaderSpecificProfiles.
sslConnection	boolean		JDBC driver property: sslConnection.
streamBufferSize	int		JDBC driver property: streamBufferSize.
stripTrailingZerosForDecimalNumbers	int • 1		JDBC driver property: stripTrailingZerosForDecimalNumbers.  2 NO 1 YES
sysSchema	string		JDBC driver property: sysSchema.
timerLevelForQueryTimeOut	int • 2 • 1 • -1		JDBC driver property: timerLevelForQueryTimeOut.  2 QUERYTIMEOUT_CONNECTION_LEVEL 1 QUERYTIMEOUT_STATEMENT_LEVEL -1 QUERYTIMEOUT_DISABLED
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceFileCount	int		JDBC driver property: traceFileCount.
traceFileSize	int		JDBC driver property: traceFileSize.
traceLevel	int	0	Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
traceOption	int • 1 • 0		JDBC driver property: traceOption  1 1 0 0

Attribute name	Data type	Default value	Description
translateForBitData	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: translateForBitData. 2 SERVER_ENCODING_REPRESENTATION 1 HEX_REPRESENTATION
updateCountForBatch	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: updateCountForBatch. 2 TOTAL_UPDATE_COUNT 1 NO_UPDATE_COUNT
useCachedCursor	boolean		JDBC driver property: useCachedCursor.
useIdentityValLocalForAutoGeneratedKeys	boolean		JDBC driver property: useIdentityValLocalForAutoGeneratedKeys.
useJDBC41DefinitionForGetColumns	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC41DefinitionForGetColumns. 2 NO 1 YES
useJDBC4ColumnNameAndLabelSemantics	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
useTransactionRedirect	boolean		JDBC driver property: useTransactionRedirect.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaNetworkOptimization	boolean		JDBC driver property: xaNetworkOptimization.

### properties.derby.client

Data source properties for Derby Network Client JDBC driver.

false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1527	Port on which to obtain database connections.
retrieveMessageText	boolean	true	JDBC driver property: retrieveMessageText.
securityMechanism	<ul style="list-style-type: none"> <li>3</li> <li>7</li> <li>4</li> <li>9</li> <li>8</li> </ul>	3	<p>JDBC driver property: securityMechanism. Values are:</p> <p>3 (CLEAR_TEXT_PASSWORD_SECURITY),</p> <p>4 (USER_ONLY_SECURITY),</p> <p>7 (ENCRYPTED_PASSWORD_SECURITY),</p> <p>8 (STRONG_PASSWORD_SUBSTITUTE_SECURITY),</p> <p>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY)</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY</p> <p>7 ENCRYPTED_PASSWORD_SECURITY</p> <p>4 USER_ONLY_SECURITY</p> <p>9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p> <p>8 STRONG_PASSWORD_SUBSTITUTE_SECURITY</p>

Attribute name	Data type	Default value	Description
serverName	string	localhost	Server where the database is running.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		JDBC driver property: shutdownDatabase. <b>false</b> Do not shut down the database. <b>shutdown</b> Shut down the database when a connection is attempted.
ssl	<ul style="list-style-type: none"> <li>basic</li> <li>off</li> <li>peerAuthentication</li> </ul>		JDBC driver property: ssl. <b>basic</b> basic <b>off</b> off <b>peerAuthentication</b> peerAuthentication
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_XA_CALLS=2048, TRACE_ALL=-1.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

### properties.derby.embedded

Data source properties for Derby Embedded JDBC driver.

false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		<p>JDBC driver property: shutdownDatabase.</p> <p><b>false</b> Do not shut down the database.</p> <p><b>shutdown</b> Shut down the database when a connection is attempted.</p>
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

### properties.informix

Data source properties for the Informix JDBC driver.

false

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
ifxCLIENT_LOCALE	string		JDBC driver property: ifxCLIENT_LOCALE.
ifxCPMAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMInitPoolSize	int		JDBC driver property: ifxCPMInitPoolSize.
ifxCPMMaxConnections	int		JDBC driver property: ifxCPMMaxConnections.
ifxCPMMaxPoolSize	int		JDBC driver property: ifxCPMMaxPoolSize.
ifxCPMMinAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMMinAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMMinPoolSize	int		JDBC driver property: ifxCPMMinPoolSize.
ifxCPMServiceInterval	A period of time with millisecond precision		JDBC driver property: ifxCPMServiceInterval. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxDBANSIWARN	boolean		JDBC driver property: ifxDBANSIWARN.
ifxDBCENTURY	string		JDBC driver property: ifxDBCENTURY.
ifxDBDATE	string		JDBC driver property: ifxDBDATE.
ifxDBSPACETEMP	string		JDBC driver property: ifxDBSPACETEMP.

Attribute name	Data type	Default value	Description
ifxDBTEMP	string		JDBC driver property: ifxDBTEMP.
ifxDBTIME	string		JDBC driver property: ifxDBTIME.
ifxDBUPSPACE	string		JDBC driver property: ifxDBUPSPACE.
ifxDB_LOCALE	string		JDBC driver property: ifxDB_LOCALE.
ifxDELIMIDENT	boolean		JDBC driver property: ifxDELIMIDENT.
ifxENABLE_TYPE_CACHE	boolean		JDBC driver property: ifxENABLE_TYPE_CACHE.
ifxFET_BUF_SIZE	int		JDBC driver property: ifxFET_BUF_SIZE.
ifxGL_DATE	string		JDBC driver property: ifxGL_DATE.
ifxGL_DATETIME	string		JDBC driver property: ifxGL_DATETIME.
ifxIFXHOST	string	localhost	JDBC driver property: ifxIFXHOST.
ifxIFX_AUTOFREE	boolean		JDBC driver property: ifxIFX_AUTOFREE.
ifxIFX_DIRECTIVES	string		JDBC driver property: ifxIFX_DIRECTIVES.
ifxIFX_LOCK_MODE_WAIT	A period of time with second precision	2s	JDBC driver property: ifxIFX_LOCK_MODE_WAIT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxIFX_SOC_TIMEOUT	A period of time with millisecond precision		JDBC driver property: ifxIFX_SOC_TIMEOUT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxIFX_USEPUT	boolean		JDBC driver property: ifxIFX_USEPUT.

Attribute name	Data type	Default value	Description
ifxIFX_USE_STRENC	boolean		JDBC driver property: ifxIFX_USE_STRENC.
ifxIFX_XASPEC	string	y	JDBC driver property: ifxIFX_XASPEC.
ifxINFORMIXCONRETRY	int		JDBC driver property: ifxINFORMIXCONRETRY.
ifxINFORMIXCONTIME	A period of time with second precision		JDBC driver property: ifxINFORMIXCONTIME. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxINFORMIXOPCACHE	string		JDBC driver property: ifxINFORMIXOPCACHE.
ifxINFORMIXSTACKSIZE	int		JDBC driver property: ifxINFORMIXSTACKSIZE.
ifxJDBCTEMP	string		JDBC driver property: ifxJDBCTEMP.
ifxLDAP_IFXBASE	string		JDBC driver property: ifxLDAP_IFXBASE.
ifxLDAP_PASSWD	string		JDBC driver property: ifxLDAP_PASSWD.
ifxLDAP_URL	string		JDBC driver property: ifxLDAP_URL.
ifxLDAP_USER	string		JDBC driver property: ifxLDAP_USER.
ifxLOBCACHE	int		JDBC driver property: ifxLOBCACHE.
ifxNEWCODESET	string		JDBC driver property: ifxNEWCODESET.
ifxNEWLOCALE	string		JDBC driver property: ifxNEWLOCALE.
ifxNODEFDAC	string		JDBC driver property: ifxNODEFDAC.
ifxOPTCOMPIND	string		JDBC driver property: ifxOPTCOMPIND.
ifxOPTOFC	string		JDBC driver property: ifxOPTOFC.
ifxOPT_GOAL	string		JDBC driver property: ifxOPT_GOAL.
ifxPATH	string		JDBC driver property: ifxPATH.
ifxPDQPRIORITY	string		JDBC driver property: ifxPDQPRIORITY.

Attribute name	Data type	Default value	Description
ifxPLCONFIG	string		JDBC driver property: ifxPLCONFIG.
ifxPLOAD_LO_PATH	string		JDBC driver property: ifxPLOAD_LO_PATH.
ifxPROTOCOLTRACE	int		JDBC driver property: ifxPROTOCOLTRACE.
ifxPROTOCOLTRACEFILE	string		JDBC driver property: ifxPROTOCOLTRACEFILE.
ifxPROXY	string		JDBC driver property: ifxPROXY.
ifxPSORT_DBTEMP	string		JDBC driver property: ifxPSORT_DBTEMP.
ifxPSORT_NPROCS	boolean		JDBC driver property: ifxPSORT_NPROCS.
ifxSECURITY	string		JDBC driver property: ifxSECURITY.
ifxSQLH_FILE	string		JDBC driver property: ifxSQLH_FILE.
ifxSQLH_LOC	string		JDBC driver property: ifxSQLH_LOC.
ifxSQLH_TYPE	string		JDBC driver property: ifxSQLH_TYPE.
ifxSSLCONNECTION	string		JDBC driver property: ifxSSLCONNECTION.
ifxSTMT_CACHE	string		JDBC driver property: ifxSTMT_CACHE.
ifxTRACE	int		JDBC driver property: ifxTRACE.
ifxTRACEFILE	string		JDBC driver property: ifxTRACEFILE.
ifxTRUSTED_CONTEXT	string		JDBC driver property: ifxTRUSTED_CONTEXT.
ifxUSEV5SERVER	boolean		JDBC driver property: ifxUSEV5SERVER.
ifxUSE_DTENV	boolean		JDBC driver property: ifxUSE_DTENV.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
roleName	string		JDBC driver property: roleName.
serverName	string		Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

### properties.informix.jcc

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for Informix.

false

Attribute name	Data type	Default value	Description
DBANSIWARN	boolean		JDBC driver property: DBANSIWARN.
DBDATE	string		JDBC driver property: DBDATE.
DBPATH	string		JDBC driver property: DBPATH.
DBSPACETEMP	string		JDBC driver property: DBSPACETEMP.
DBTEMP	string		JDBC driver property: DBTEMP.
DBUPSPACE	string		JDBC driver property: DBUPSPACE.
DELIMIDENT	boolean		JDBC driver property: DELIMIDENT.
IFX_DIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_DIRECTIVES. ON ON OFF OFF
IFX_EXTDIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_EXTDIRECTIVES. ON ON OFF OFF
IFX_UPDDESC	string		JDBC driver property: IFX_UPDDESC.

Attribute name	Data type	Default value	Description
IFX_XASTDCOMPLIANCE_XAEND	<ul style="list-style-type: none"> <li>0</li> </ul>		JDBC driver property: IFX_XASTDCOMPLIANCE_XAEND. <b>1</b> 1 <b>0</b> 0
INFORMIXOPCACHE	string		JDBC driver property: INFORMIXOPCACHE.
INFORMIXSTACKSIZE	string		JDBC driver property: INFORMIXSTACKSIZE.
NODEFDAC	<ul style="list-style-type: none"> <li>yes</li> <li>no</li> </ul>		JDBC driver property: NODEFDAC. <b>yes</b> yes <b>no</b> no
OPTCOMPIND	<ul style="list-style-type: none"> <li>2</li> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTCOMPIND. <b>2</b> 2 <b>1</b> 1 <b>0</b> 0
OPTOFC	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTOFC. <b>1</b> 1 <b>0</b> 0
PDQPRIORITY	<ul style="list-style-type: none"> <li>HIGH</li> <li>LOW</li> <li>OFF</li> </ul>		JDBC driver property: PDQPRIORITY. <b>HIGH</b> HIGH <b>LOW</b> LOW <b>OFF</b> OFF
PSORT_DBTEMP	string		JDBC driver property: PSORT_DBTEMP.
PSORT_NPROCS	string Maximum: 10		JDBC driver property: PSORT_NPROCS.
STMT_CACHE	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: STMT_CACHE. <b>1</b> 1 <b>0</b> 0
currentLockTimeout	A period of time with second precision	2s	JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean		JDBC driver property: deferPrepares.
driverType	int	4	JDBC driver property: driverType.
enableNamedParameterMarkers	int		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO).
enableSeamlessFailover	int		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO).
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.
keepDynamic	int		JDBC driver property: keepDynamic.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
progressiveStreaming	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		JDBC driver property: progressiveStreaming. Values are: 1 (YES) or 2 (NO).  2      NO 1      YES
queryDataSize	int  Minimum: 4096  Maximum: 10485760		JDBC driver property: queryDataSize.

Attribute name	Data type	Default value	Description
resultSetHoldability	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
retrieveMessagesFromServerOnGetMessage	boolean	true	JDBC driver property: retrieveMessagesFromServerOnGetMessage.
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 9</li> </ul>		<p>JDBC driver property: securityMechanism. Values are: 3 (CLEAR_TEXT_PASSWORD_SECURITY), 4 (USER_ONLY_SECURITY), 7 (ENCRYPTED_PASSWORD_SECURITY), 9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY).</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY 7 ENCRYPTED_PASSWORD_SECURITY 4 USER_ONLY_SECURITY 9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p>
serverName	string	localhost	Server where the database is running.
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.

Attribute name	Data type	Default value	Description
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
useJDBC4ColumnNameAndLabelSemantics	boolean		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO).
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

### properties.microsoft.sqlserver

Data source properties for Microsoft SQL Server JDBC Driver.

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database. Example: jdbc:sqlserver://localhost:1433;databaseName=myDB.
applicationIntent	<ul style="list-style-type: none"> <li>ReadOnly</li> <li>ReadWrite</li> </ul>		JDBC driver property: applicationIntent. <b>ReadOnly</b> ReadOnly <b>ReadWrite</b> ReadWrite
applicationName	string		JDBC driver property: applicationName.
authenticationScheme	<ul style="list-style-type: none"> <li>NativeAuthentication</li> <li>JavaKerberos</li> </ul>		JDBC driver property: authenticationScheme. <b>NativeAuthentication</b> NativeAuthentication <b>JavaKerberos</b> JavaKerberos

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
encrypt	boolean		JDBC driver property: encrypt.
failoverPartner	string		JDBC driver property: failoverPartner.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
instanceName	string		JDBC driver property: instanceName.
integratedSecurity	boolean		JDBC driver property: integratedSecurity.
lastUpdateCount	boolean		JDBC driver property: lastUpdateCount.
lockTimeout	A period of time with millisecond precision		JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
multiSubnetFailover	boolean		JDBC driver property: multiSubnetFailover.
packetSize	int Minimum: 512 Maximum: 32767		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.

Attribute name	Data type	Default value	Description
responseBuffering	<ul style="list-style-type: none"> <li>full</li> <li>adaptive</li> </ul>		JDBC driver property: responseBuffering. <b>full</b> full <b>adaptive</b> adaptive
selectMethod	<ul style="list-style-type: none"> <li>direct</li> <li>cursor</li> </ul>		JDBC driver property: selectMethod. <b>direct</b> direct <b>cursor</b> cursor
sendStringParametersAsUnicode	boolean	false	JDBC driver property: sendStringParametersAsUnicode.
sendTimeAsDatetime	boolean		JDBC driver property: sendTimeAsDatetime.
serverName	string	localhost	Server where the database is running.
trustServerCertificate	boolean		JDBC driver property: trustServerCertificate.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
workstationID	string		JDBC driver property: workstationID.
xopenStates	boolean		JDBC driver property: xopenStates.

### properties.oracle

Data source properties for Oracle JDBC driver.

false

Attribute name	Data type	Default value	Description
ONSConfiguration	string		JDBC driver property: ONSConfiguration.
TNSEntryName	string		JDBC driver property: TNSEntryName.
URL	string		URL for connecting to the database. Examples: jdbc:oracle:thin://localhost:1521/sample or jdbc:oracle:oci://localhost:1521/sample.
connectionProperties	string		JDBC driver property: connectionProperties.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
driverType	<ul style="list-style-type: none"> <li>oci</li> <li>thin</li> </ul>	thin	JDBC driver property: driverType.  <b>oci</b> oci <b>thin</b> thin
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	string		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1521	Port on which to obtain database connections.
serverName	string	localhost	Server where the database is running.
serviceName	string		JDBC driver property: serviceName.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**properties.sybase**

Data source properties for Sybase JDBC driver.

false

Attribute name	Data type	Default value	Description
SERVER_INITIATED_TRANSACTIONS	<ul style="list-style-type: none"> <li>false</li> <li>true</li> </ul>	false	JDBC driver property: SERVER_INITIATED_TRANSACTIONS.  <b>false</b> false <b>true</b> true
connectionProperties	string	SELECT_OPENS_CURSOR=true	JDBC driver property: connectionProperties.
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	<ul style="list-style-type: none"> <li>• SSL</li> <li>• socket</li> </ul>		JDBC driver property: networkProtocol.  <b>SSL</b> SSL <b>socket</b> socket
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	5000	Port on which to obtain database connections.
resourceManagerName	string		JDBC driver property: resourceManagerName.
serverName	string	localhost	Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
version	int		JDBC driver property: version.

#### recoveryAuthData

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## Database Store (databaseStore)

Specifies a relational database as a persistent store for server features.

- authData
- dataSource
  - connectionManager
  - containerAuthData
  - jaasLoginContextEntry
  - jdbcDriver
    - library
      - file
      - fileset
      - folder
  - properties
  - properties.datadirect.sqlserver
  - properties.db2.i.native
  - properties.db2.i.toolbox
  - properties.db2.jcc
  - properties.derby.client
  - properties.derby.embedded
  - properties.informix
  - properties.informix.jcc
  - properties.microsoft.sqlserver
  - properties.oracle
  - properties.sybase
  - recoveryAuthData

Attribute name	Data type	Default value	Description
authDataRef	A reference to top level authData element (string).		Authentication data for task scheduling, queries, and execution.
createTables	boolean	true	When set to true, database tables are created.
dataSourceRef	A reference to top level dataSource element (string).	DefaultDataSource	Data source that connects to the persistent store.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
keyGenerationStrategy	<ul style="list-style-type: none"> <li>• TABLE</li> <li>• SEQUENCE</li> <li>• IDENTITY</li> <li>• AUTO</li> </ul>	AUTO	<p>The preferred strategy for generating unique primary keys. If the selected strategy is not supported for the database, a different strategy might be used.</p> <p><b>TABLE</b> Use a database table to generate unique primary keys.</p> <p><b>SEQUENCE</b> Use a database sequence to generate unique primary keys.</p> <p><b>IDENTITY</b> Use a database identity column to generate unique primary keys.</p> <p><b>AUTO</b> Automatically select the strategy to generate unique primary keys.</p>
schema	string		Schema name with read and write access to the database tables.
tablePrefix	string	WLP	Name prefix for tables, sequences, and other database artifacts.

#### authData

Authentication data for task scheduling, queries, and execution.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

#### dataSource

Data source that connects to the persistent store.

false

Attribute name	Data type	Default value	Description
beginTranForResultSetScrolling	boolean	true	Attempt transaction enlistment when result set scrolling interfaces are used.
beginTranForVendorAPIs	boolean	true	Attempt transaction enlistment when vendor interfaces are used.
commitOrRollbackOnCleanup	<ul style="list-style-type: none"> <li>• commit</li> <li>• rollback</li> </ul>		<p>Determines how to clean up connections that might be in a database unit of work (AutoCommit=false) when the connection is closed or returned to the pool.</p> <p><b>commit</b> Clean up the connection by committing.</p> <p><b>rollback</b> Clean up the connection by rolling back.</p>
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a data source.
connectionSharing	<ul style="list-style-type: none"> <li>• MatchOriginalRequest</li> <li>• MatchCurrentState</li> </ul>	MatchOriginalRequest	<p>Specifies how connections are matched for sharing.</p> <p><b>MatchOriginalRequest</b> When sharing connections, match based on the original connection request.</p> <p><b>MatchCurrentState</b> When sharing connections, match based on the current state of the connection.</p>
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

Attribute name	Data type	Default value	Description
enableConnectionCasting	boolean	false	Indicates that connections obtained from the data source should be castable to interface classes that the JDBC vendor connection implementation implements. Enabling this option incurs additional overhead on each getConnection operation. If vendor JDBC interfaces are needed less frequently, it might be more efficient to leave this option disabled and use Connection.unwrap(interface) only where it is needed.
isolationLevel	<ul style="list-style-type: none"> <li>• TRANSACTION_REPEATABLE_READ</li> <li>• TRANSACTION_READ_COMMITTED</li> <li>• TRANSACTION_SERIALIZABLE</li> <li>• TRANSACTION_READ_UNCOMMITTED</li> <li>• TRANSACTION_SNAPSHOT</li> </ul>		<p>Default transaction isolation level.</p> <p><b>TRANSACTION_REPEATABLE_READ</b> Dirty reads and non-repeatable reads are prevented; phantom reads can occur.</p> <p><b>TRANSACTION_READ_COMMITTED</b> Dirty reads are prevented; non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SERIALIZABLE</b> Dirty reads, non-repeatable reads and phantom reads are prevented.</p> <p><b>TRANSACTION_READ_UNCOMMITTED</b> Dirty reads, non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SNAPSHOT</b> Snapshot isolation for Microsoft SQL Server JDBC Driver and DataDirect Connect for JDBC driver.</p>

Attribute name	Data type	Default value	Description
jaasLoginContextEntryRef	A reference to top level jaasLoginContextEntry element (string).		JAAS login context entry for authentication.
jdbcDriverRef	A reference to top level jdbcDriver element (string).		JDBC driver for a data source.
jndiName	string		JNDI name for a data source.
queryTimeout	A period of time with second precision		Default query timeout for SQL statements. In a JTA transaction, syncQueryTimeoutWithTransactionTimeout can override this default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.
statementCacheSize	int Minimum: 0	10	Maximum number of cached statements per connection.
supplementalJDBCTrace	boolean		Supplements the JDBC driver trace that is logged when JDBC driver trace is enabled in bootstrap.properties. JDBC driver trace specifications include: com.ibm.ws.database.logwriter, com.ibm.ws.db2.logwriter, com.ibm.ws.derby.logwriter, com.ibm.ws.informix.logwriter, com.ibm.ws.oracle.logwriter, com.ibm.ws.sqlserver.logwriter, com.ibm.ws.sybase.logwriter
syncQueryTimeoutWithTransactionTimeout	boolean	false	Use the time remaining (if any) in a JTA transaction as the default query timeout for SQL statements.
transactional	boolean	true	Enable participation in transactions that are managed by the application server.

Attribute name	Data type	Default value	Description
type	<ul style="list-style-type: none"> <li>javax.sql.DataSource</li> <li>javax.sql.XADataSource</li> <li>javax.sql.ConnectionPoolDataSource</li> </ul>		Type of data source. <b>javax.sql.DataSource</b> javax.sql.DataSource <b>javax.sql.XADataSource</b> javax.sql.XADataSource <b>javax.sql.ConnectionPoolDataSource</b> javax.sql.ConnectionPoolDataSource

### dataSource > connectionManager

Connection manager for a data source.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.

Attribute name	Data type	Default value	Description
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.

Attribute name	Data type	Default value	Description
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**dataSource > containerAuthData**

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

**dataSource > jaasLoginContextEntry**

JAAS login context entry for authentication.

false

Attribute name	Data type	Default value	Description
loginModuleRef	List of references to top level jaasLoginModule elements (comma-separated string).	hashtable,userNameAndPassword,certificateURL	Word certificateURL of a JAAS login module.
name	string		Name of a JAAS configuration entry.

**dataSource > jdbcDriver**

JDBC driver for a data source.

false

Attribute name	Data type	Default value	Description
javax.sql.ConnectionPoolDataSource	string		JDBC driver implementation of javax.sql.ConnectionPoolDataSource.
javax.sql.DataSource	string		JDBC driver implementation of javax.sql.DataSource.
javax.sql.XADataSource	string		JDBC driver implementation of javax.sql.XADataSource.
libraryRef	A reference to top level library element (string).		Identifies JDBC driver JARs and native files.

**dataSource > jdbcDriver > library**

Identifies JDBC driver JARs and native files.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

**dataSource > jdbcDriver > library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**dataSource > jdbcDriver > library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**dataSource > jdbcDriver > library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**dataSource > properties**

List of JDBC vendor properties for the data source. For example, databaseName="dbname" serverName="localhost" portNumber="50000".

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database.
databaseName	string		JDBC driver property: databaseName.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
serverName	string		Server where the database is running.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**dataSource > properties.datadirect.sqlserver**

Data source properties for the DataDirect Connect for JDBC driver for Microsoft SQL Server.

false

Attribute name	Data type	Default value	Description
JDBCBehavior	<ul style="list-style-type: none"> <li>• 1</li> <li>• 0</li> </ul>	0	JDBC driver property: JDBCBehavior. Values are: 0 (JDBC 4.0) or 1 (JDBC 3.0).  <b>1</b> JDBC 3.0 <b>0</b> JDBC 4.0
XATransactionGroup	string		JDBC driver property: XATransactionGroup.
XMLDescribeType	<ul style="list-style-type: none"> <li>• longvarbinary</li> <li>• longvarchar</li> </ul>		JDBC driver property: XMLDescribeType.  <b>longvarbinary</b> longvarbinary  <b>longvarchar</b> longvarchar
accountingInfo	string		JDBC driver property: accountingInfo.
alternateServers	string		JDBC driver property: alternateServers.
alwaysReportTriggerResults	boolean		JDBC driver property: alwaysReportTriggerResults.
applicationName	string		JDBC driver property: applicationName.
authenticationMethod	<ul style="list-style-type: none"> <li>• ntlm</li> <li>• userIdPassword</li> <li>• kerberos</li> <li>• auto</li> </ul>		JDBC driver property: authenticationMethod.  <b>ntlm</b> ntlm  <b>userIdPassword</b> userIdPassword  <b>kerberos</b> kerberos  <b>auto</b> auto
bulkLoadBatchSize	long		JDBC driver property: bulkLoadBatchSize.
bulkLoadOptions	long		JDBC driver property: bulkLoadOptions.
clientHostName	string		JDBC driver property: clientHostName.
clientUser	string		JDBC driver property: clientUser.

Attribute name	Data type	Default value	Description
codePageOverride	string		JDBC driver property: codePageOverride.
connectionRetryCount	int		JDBC driver property: connectionRetryCount.
connectionRetryDelay	A period of time with second precision		JDBC driver property: connectionRetryDelay. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
convertNull	int		JDBC driver property: convertNull.
databaseName	string		JDBC driver property: databaseName.
dateTimeInputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeInputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
dateTimeOutputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeOutputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
describeInputParameters	<ul style="list-style-type: none"> <li>• describeIfString</li> <li>• noDescribe</li> <li>• describeIfDateTime</li> <li>• describeAll</li> </ul>		JDBC driver property: describeInputParameters.  <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll

Attribute name	Data type	Default value	Description
describeOutputParameters	<ul style="list-style-type: none"> <li>describeIfString</li> <li>noDescribe</li> <li>describeIfDateTime</li> <li>describeAll</li> </ul>		JDBC driver property: describeOutputParameters. <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll
enableBulkLoad	boolean		JDBC driver property: enableBulkLoad.
enableCancelTimeout	boolean		JDBC driver property: enableCancelTimeout.
encryptionMethod	<ul style="list-style-type: none"> <li>loginSSL</li> <li>requestSSL</li> <li>SSL</li> <li>noEncryption</li> </ul>		JDBC driver property: encryptionMethod. <b>loginSSL</b> loginSSL <b>requestSSL</b> requestSSL <b>SSL</b> SSL <b>noEncryption</b> noEncryption
failoverGranularity	<ul style="list-style-type: none"> <li>disableIntegrityCheck</li> <li>atomicWithRepositioning</li> <li>nonAtomic</li> <li>atomic</li> </ul>		JDBC driver property: failoverGranularity. <b>disableIntegrityCheck</b> disableIntegrityCheck <b>atomicWithRepositioning</b> atomicWithRepositioning <b>nonAtomic</b> nonAtomic <b>atomic</b> atomic
failoverMode	<ul style="list-style-type: none"> <li>connect</li> <li>select</li> <li>extended</li> </ul>		JDBC driver property: failoverMode. <b>connect</b> connect <b>select</b> select <b>extended</b> extended
failoverPreconnect	boolean		JDBC driver property: failoverPreconnect.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
initializationString	string		JDBC driver property: initializationString.
insensitiveResultSetBufferSize	int		JDBC driver property: insensitiveResultSetBufferSize.

Attribute name	Data type	Default value	Description
javaDoubleToString	boolean		JDBC driver property: javaDoubleToString.
loadBalancing	boolean		JDBC driver property: loadBalancing.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
longDataCacheSize	int Minimum: -1		JDBC driver property: longDataCacheSize.
netAddress	string		JDBC driver property: netAddress.
packetSize	int Minimum: -1 Maximum: 128		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
queryTimeout	A period of time with second precision		JDBC driver property: queryTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
resultsetMetaDataOptions	int		JDBC driver property: resultSetMetaDataOptions.
selectMethod	<ul style="list-style-type: none"> <li>• direct</li> <li>• cursor</li> </ul>		JDBC driver property: selectMethod.  <b>direct</b> direct <b>cursor</b> cursor
serverName	string	localhost	Server where the database is running.
snapshotSerializable	boolean		JDBC driver property: snapshotSerializable.

Attribute name	Data type	Default value	Description
spyAttributes	string		JDBC driver property: spyAttributes.
stringInputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringInputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
stringOutputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringOutputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
suppressConnectionWarnings	boolean		JDBC driver property: suppressConnectionWarnings.
transactionMode	<ul style="list-style-type: none"> <li>explicit</li> <li>implicit</li> </ul>		JDBC driver property: transactionMode. <b>explicit</b> explicit <b>implicit</b> implicit
truncateFractionalSeconds	boolean		JDBC driver property: truncateFractionalSeconds.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
useServerSideUpdatableCursors	boolean		JDBC driver property: useServerSideUpdatableCursors.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
validateServerCertificate	boolean		JDBC driver property: validateServerCertificate.

#### dataSource > properties.db2.i.native

Data source properties for the IBM DB2 for i Native JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>read only</li> <li>all</li> <li>read call</li> </ul>	all	JDBC driver property: access. <b>read only</b> read only <b>all</b> all <b>read call</b> read call

Attribute name	Data type	Default value	Description
autoCommit	boolean	true	JDBC driver property: autoCommit.
batchStyle	<ul style="list-style-type: none"> <li>• 2.1</li> <li>• 2.0</li> </ul>	2.0	JDBC driver property: batchStyle. <b>2.1</b> 2.1 <b>2.0</b> 2.0
behaviorOverride	int		JDBC driver property: behaviorOverride.
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive
dataTruncation	string	true	JDBC driver property: dataTruncation.
databaseName	string	*LOCAL	JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy
dateSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		JDBC driver property: dateSeparator. <b>\,</b> The comma character (,). <b>b</b> The character b <b>.</b> The period character (.). <b>/</b> The forward slash character (/). <b>-</b> The dash character (-).
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		JDBC driver property: decimalSeparator. <b>\,</b> The comma character (,). <b>.</b> The period character (.).
directMap	boolean	true	JDBC driver property: directMap.
doEscapeProcessing	boolean	true	JDBC driver property: doEscapeProcessing.
fullErrors	boolean		JDBC driver property: fullErrors.
libraries	string		JDBC driver property: libraries.
lobThreshold	int Maximum: 500000	0	JDBC driver property: lobThreshold.

Attribute name	Data type	Default value	Description
lockTimeout	A period of time with second precision	0	JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>• 31</li> <li>• 63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 63
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
networkProtocol	int		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
prefetch	boolean	true	JDBC driver property: prefetch.
queryOptimizeGoal	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>	2	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).  <b>2</b> *ALLIO <b>1</b> *FIRSTIO

Attribute name	Data type	Default value	Description
reuseObjects	boolean	true	JDBC driver property: reuseObjects.
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
systemNaming	boolean	false	JDBC driver property: systemNaming.
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat.  <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  \,    The comma character (,). <b>b</b> The character b :    The colon character (:). .    The period character (.).
trace	boolean		JDBC driver property: trace.
transactionTimeout	A period of time with second precision	0	JDBC driver property: transactionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateHex	<ul style="list-style-type: none"> <li>• binary</li> <li>• character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
useBlockInsert	boolean	false	JDBC driver property: useBlockInsert.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**dataSource > properties.db2.i.toolbox**

Data source properties for the IBM DB2 for i Toolbox JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>• read only</li> <li>• all</li> <li>• read call</li> </ul>	all	JDBC driver property: access.  <b>read only</b> read only  <b>all</b> all  <b>read call</b> read call
behaviorOverride	int		JDBC driver property: behaviorOverride.
bidiImplicitReordering	boolean	true	JDBC driver property: bidiImplicitReordering.
bidiNumericOrdering	boolean	false	JDBC driver property: bidiNumericOrdering.
bidiStringType	int		JDBC driver property: bidiStringType.
bigDecimal	boolean	true	JDBC driver property: bigDecimal.
blockCriteria	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>	2	JDBC driver property: blockCriteria. Values are: 0 (no record blocking), 1 (block if FOR FETCH ONLY is specified), 2 (block if FOR UPDATE is specified).  <b>2</b> 2  <b>1</b> 1  <b>0</b> 0

Attribute name	Data type	Default value	Description
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> <li>• insensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive <b>insensitive</b> insensitive
dataCompression	boolean	true	JDBC driver property: dataCompression.
dataTruncation	boolean	true	JDBC driver property: dataTruncation.
databaseName	string		JDBC driver property: databaseName.
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy

Attribute name	Data type	Default value	Description
dateSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		<p>JDBC driver property: dateSeparator.</p> <p>The space character ( ).</p> <p>\, The comma character (,).</p> <p>. The period character (.).</p> <p>/ The forward slash character (/).</p> <p>- The dash character (-).</p>
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		<p>JDBC driver property: decimalSeparator.</p> <p>\, The comma character (,).</p> <p>. The period character (.).</p>
driver	<ul style="list-style-type: none"> <li>• toolbox</li> <li>• native</li> </ul>	toolbox	<p>JDBC driver property: driver.</p> <p><b>toolbox</b> toolbox</p> <p><b>native</b> native</p>
errors	<ul style="list-style-type: none"> <li>• full</li> <li>• basic</li> </ul>	basic	<p>JDBC driver property: errors.</p> <p><b>full</b> full</p> <p><b>basic</b> basic</p>
extendedDynamic	boolean	false	JDBC driver property: extendedDynamic.
extendedMetaData	boolean	false	JDBC driver property: extendedMetaData.
fullOpen	boolean	false	JDBC driver property: fullOpen.
holdInputLocators	boolean	true	JDBC driver property: holdInputLocators.
holdStatements	boolean	false	JDBC driver property: holdStatements.
isolationLevelSwitchingSupport	boolean	false	JDBC driver property: isolationLevelSwitchingSupport.
keepAlive	boolean		JDBC driver property: keepAlive.
lazyClose	boolean	false	JDBC driver property: lazyClose.
libraries	string		JDBC driver property: libraries.

Attribute name	Data type	Default value	Description
lobThreshold	int Minimum: 0 Maximum: 16777216	0	JDBC driver property: lobThreshold.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>• 31</li> <li>• 63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 64
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
metaDataSource	int Minimum: 0 Maximum: 1	1	JDBC driver property: metaDataSource.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
naming	<ul style="list-style-type: none"> <li>• system</li> <li>• sql</li> </ul>	sql	JDBC driver property: naming.  <b>system</b> system <b>sql</b> sql
package	string		JDBC driver property: package.
packageAdd	boolean	true	JDBC driver property: packageAdd.
packageCCSID	<ul style="list-style-type: none"> <li>• 13488</li> <li>• 1200</li> </ul>	13488	JDBC driver property: packageCCSID. Values are: 1200 (UCS-2) or 13488 (UTF-16).  <b>13488</b> 13488 (UTF-16) <b>1200</b> 1200 (UCS-2)
packageCache	boolean	false	JDBC driver property: packageCache.

Attribute name	Data type	Default value	Description
packageCriteria	<ul style="list-style-type: none"> <li>default</li> <li>select</li> </ul>	default	JDBC driver property: packageCriteria. <b>default</b> default <b>select</b> select
packageError	<ul style="list-style-type: none"> <li>exception</li> <li>none</li> <li>warning</li> </ul>	warning	JDBC driver property: packageError. <b>exception</b> exception <b>none</b> none <b>warning</b> warning
packageLibrary	string	QGPL	JDBC driver property: packageLibrary.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
prefetch	boolean	true	JDBC driver property: prefetch.
prompt	boolean	false	JDBC driver property: prompt.
proxyServer	string		JDBC driver property: proxyServer.
qaqqiniLibrary	string		JDBC driver property: qaqqiniLibrary.
queryOptimizeGoal	int Minimum: 0 Maximum: 2	0	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).
receiveBufferSize	int Minimum: 1		JDBC driver property: receiveBufferSize.
remarks	<ul style="list-style-type: none"> <li>system</li> <li>sql</li> </ul>	system	JDBC driver property: remarks. <b>system</b> system <b>sql</b> sql
rollbackCursorHold	boolean	false	JDBC driver property: rollbackCursorHold.
savePasswordWhenSerialized	boolean	false	JDBC driver property: savePasswordWhenSerialized.
secondaryUrl	string		JDBC driver property: secondaryUrl.
secure	boolean	false	JDBC driver property: secure.
sendBufferSize	int Minimum: 1		JDBC driver property: sendBufferSize.

Attribute name	Data type	Default value	Description
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
soLinger	A period of time with second precision		JDBC driver property: soLinger. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
soTimeout	A period of time with millisecond precision		JDBC driver property: soTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
sort	<ul style="list-style-type: none"> <li>• hex</li> <li>• table</li> <li>• language</li> </ul>	hex	JDBC driver property: sort. <b>hex</b> hex <b>table</b> table <b>language</b> language
sortLanguage	string		JDBC driver property: sortLanguage.
sortTable	string		JDBC driver property: sortTable.
sortWeight	<ul style="list-style-type: none"> <li>• unqiue</li> <li>• shared</li> </ul>		JDBC driver property: sortWeight. <b>unqiue</b> unique <b>shared</b> shared
tcpNoDelay	boolean		JDBC driver property: tcpNoDelay.
threadUsed	boolean	true	JDBC driver property: threadUsed.

Attribute name	Data type	Default value	Description
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat. <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  The space character ( ). \, The comma character (,). : The colon character (:). . The period character (.).
toolboxTrace	<ul style="list-style-type: none"> <li>• diagnostic</li> <li>• information</li> <li>• conversion</li> <li>• error</li> <li>• thread</li> <li>• proxy</li> <li>• none</li> <li>• datastream</li> <li>• pcml</li> <li>• all</li> <li>• jdbc</li> <li>• warning</li> </ul>		JDBC driver property: toolboxTrace. <b>diagnostic</b> diagnostic <b>information</b> information <b>conversion</b> conversion <b>error</b> error <b>thread</b> thread <b>proxy</b> proxy <b>none</b> none <b>datastream</b> datastream <b>pcml</b> pcml <b>all</b> all <b>jdbc</b> jdbc <b>warning</b> warning
trace	boolean		JDBC driver property: trace.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateBoolean	boolean	true	JDBC driver property: translateBoolean.

Attribute name	Data type	Default value	Description
translateHex	<ul style="list-style-type: none"> <li>binary</li> <li>character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
trueAutoCommit	boolean	false	JDBC driver property: trueAutoCommit.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaLooselyCoupledSupport	int  Minimum: 0  Maximum: 1	0	JDBC driver property: xaLooselyCoupledSupport.

#### dataSource > properties.db2.jcc

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for DB2.

false

Attribute name	Data type	Default value	Description
activateDatabase	int		JDBC driver property: activateDatabase.
alternateGroupDatabaseName	string		JDBC driver property: alternateGroupDatabaseName.
alternateGroupPortNumber	string		JDBC driver property: alternateGroupPortNumber.
alternateGroupServerName	string		JDBC driver property: alternateGroupServerName.
blockingReadConnectionTimeout	A period of time with second precision		JDBC driver property: blockingReadConnectionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
clientAccountingInformation	string		JDBC driver property: clientAccountingInformation.
clientApplicationInformation	string		JDBC driver property: clientApplicationInformation.
clientRerouteAlternatePortNumber	string		JDBC driver property: clientRerouteAlternatePortNumber.
clientRerouteAlternateServerName	string		JDBC driver property: clientRerouteAlternateServerName.

Attribute name	Data type	Default value	Description
clientUser	string		JDBC driver property: clientUser.
clientWorkstation	string		JDBC driver property: clientWorkstation.
connectionCloseWithInFlightTransaction	Transaction <ul style="list-style-type: none"> <li>• 1</li> </ul>		JDBC driver property: connectionCloseWithInFlightTransaction. 2 CONNECTION_CLOSE_WITH_ROLLBACK 1 CONNECTION_CLOSE_WITH_EXCEPTION
currentAlternateGroupEntry	int		JDBC driver property: currentAlternateGroupEntry.
currentFunctionPath	string		JDBC driver property: currentFunctionPath.
currentLocaleLcCtype	string		JDBC driver property: currentLocaleLcCtype.
currentLockTimeout	A period of time with second precision		JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
currentPackagePath	string		JDBC driver property: currentPackagePath.
currentPackageSet	string		JDBC driver property: currentPackageSet.
currentSQLID	string		JDBC driver property: currentSQLID.
currentSchema	string		JDBC driver property: currentSchema.
cursorSensitivity	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). 2 TYPE_SCROLL_ASENSITIVE 1 TYPE_SCROLL_SENSITIVE_DYNAMIC 0 TYPE_SCROLL_SENSITIVE_STATIC
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean	true	JDBC driver property: deferPrepares.

Attribute name	Data type	Default value	Description
driverType	<ul style="list-style-type: none"> <li>2</li> <li>4</li> </ul>	4	JDBC driver property: driverType. 2 Type 2 JDBC driver. 4 Type 4 JDBC driver.
enableAlternateGroupSeamlessACR	boolean		JDBC driver property: enableAlternateGroupSeamlessACR.
enableClientAffinitiesList	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableClientAffinitiesList. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableExtendedDescribe	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedDescribe. 2 NO 1 YES
enableExtendedIndicators	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedIndicators. 2 NO 1 YES
enableNamedParameterMarkers	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSeamlessFailover	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeInputStreams	boolean		JDBC driver property: fullyMaterializeInputStreams.
fullyMaterializeInputStreamsOnBatchExecution	<ul style="list-style-type: none"> <li>1</li> </ul>		JDBC driver property: fullyMaterializeInputStreamsOnBatchExecution. 2 NO 1 YES
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.

Attribute name	Data type	Default value	Description
implicitRollbackOption	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: implicitRollbackOption.</p> <p><b>2</b> IMPLICIT_ROLLBACK_OPTION_CLOSE</p> <p><b>1</b> IMPLICIT_ROLLBACK_OPTION_NO</p> <p><b>0</b> IMPLICIT_ROLLBACK_OPTION_NO</p>
interruptProcessingMode	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: interruptProcessingMode.</p> <p><b>2</b> INTERRUPT_PROCESSING_MODE_C</p> <p><b>1</b> INTERRUPT_PROCESSING_MODE_S</p> <p><b>0</b> INTERRUPT_PROCESSING_MODE_D</p>
keepAliveTimeOut	A period of time with second precision		<p>JDBC driver property: keepAliveTimeOut. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
keepDynamic	int		JDBC driver property: keepDynamic.
kerberosServerPrincipal	string		JDBC driver property: kerberosServerPrincipal.
loginTimeout	A period of time with second precision		<p>JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
maxConnCachedParamBufferSize	int		JDBC driver property: maxConnCachedParamBufferSize.
maxRetriesForClientReroute	int		JDBC driver property: maxRetriesForClientReroute.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	50000	Port on which to obtain database connections.
profileName	string		JDBC driver property: profileName.

Attribute name	Data type	Default value	Description
queryCloseImplicit	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: queryCloseImplicit. Values are: 1 (QUERY_CLOSE_IMPLICIT_YES) or 2 (QUERY_CLOSE_IMPLICIT_NO).</p> <p>2        QUERY_CLOSE_IMPLICIT_NO 1        QUERY_CLOSE_IMPLICIT_YES</p>
queryDataSize	<p>int</p> <p>Minimum: 4096</p> <p>Maximum: 65535</p>		JDBC driver property: queryDataSize.
queryTimeoutInterruptProcessingMode	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: queryTimeoutInterruptProcessingMode.</p> <p>2        INTERRUPT_PROCESSING_MODAL 1        INTERRUPT_PROCESSING_MODAL</p>
readOnly	boolean		JDBC driver property: readOnly.
recordTemporalHistory	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: recordTemporalHistory.</p> <p>2        NO 1        YES</p>
resultSetHoldability	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2        CLOSE_CURSORS_AT_COMMIT 1        HOLD_CURSORS_OVER_COMMIT</p>
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2        CLOSE_CURSORS_AT_COMMIT 1        HOLD_CURSORS_OVER_COMMIT</p>
retrieveMessagesFromServerOnGetMessage	boolean	true	JDBC driver property: retrieveMessagesFromServerOnGetMessage.

Attribute name	Data type	Default value	Description
retryIntervalForClientReroute	A period of time with second precision		JDBC driver property: retryIntervalForClientReroute. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 18</li> <li>• 15</li> <li>• 9</li> <li>• 16</li> <li>• 13</li> <li>• 11</li> <li>• 12</li> </ul>		<p>JDBC driver property: securityMechanism. Values are:</p> <ul style="list-style-type: none"> <li>3 (CLEAR_TEXT_PASSWORD_SECURITY),</li> <li>4 (USER_ONLY_SECURITY),</li> <li>7 (ENCRYPTED_PASSWORD_SECURITY),</li> <li>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY),</li> <li>11 (KERBEROS_SECURITY),</li> <li>12 (ENCRYPTED_USER_AND_DATA_SECURITY),</li> <li>13 (ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY),</li> <li>15 (PLUGIN_SECURITY),</li> <li>16 (ENCRYPTED_USER_ONLY_SECURITY),</li> <li>18 (TLS_CLIENT_CERTIFICATE_SECURITY).</li> </ul> <p>3 CLEAR_TEXT_PASSWORD_SECURITY  7 ENCRYPTED_PASSWORD_SECURITY  4 USER_ONLY_SECURITY  18 TLS_CLIENT_CERTIFICATE_SECURITY  15 PLUGIN_SECURITY  9 ENCRYPTED_USER_AND_PASSWORD_SECURITY  16 ENCRYPTED_USER_ONLY_SECURITY  13 ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY  11 KERBEROS_SECURITY  12 ENCRYPTED_USER_AND_DATA_SECURITY</p>
sendDataAsIs	boolean		JDBC driver property: sendDataAsIs.
serverName	string	localhost	Server where the database is running.
sessionTimeZone	string		JDBC driver property: sessionTimeZone.
sqljCloseStmtsWithOpenResultSet	boolean		JDBC driver property: sqljCloseStmtsWithOpenResultSet.

Attribute name	Data type	Default value	Description
sqljEnableClassLoaderSpecificProfiles	boolean		JDBC driver property: sqljEnableClassLoaderSpecificProfiles.
sslConnection	boolean		JDBC driver property: sslConnection.
streamBufferSize	int		JDBC driver property: streamBufferSize.
stripTrailingZerosForDecimalNumbers	Numbers <ul style="list-style-type: none"> <li>• 1</li> </ul>		JDBC driver property: stripTrailingZerosForDecimalNumbers. 2 NO 1 YES
sysSchema	string		JDBC driver property: sysSchema.
timerLevelForQueryTimeOut	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• -1</li> </ul>		JDBC driver property: timerLevelForQueryTimeOut. 2 QUERYTIMEOUT_CONNECTION 1 QUERYTIMEOUT_STATEMENT_L -1 QUERYTIMEOUT_DISABLED
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceFileCount	int		JDBC driver property: traceFileCount.
traceFileSize	int		JDBC driver property: traceFileSize.
traceLevel	int	0	Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
traceOption	<ul style="list-style-type: none"> <li>• 1</li> <li>• 0</li> </ul>		JDBC driver property: traceOption 1 1 0 0

Attribute name	Data type	Default value	Description
translateForBitData	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: translateForBitData. 2 SERVER_ENCODING_REPRESENTATION 1 HEX_REPRESENTATION
updateCountForBatch	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: updateCountForBatch. 2 TOTAL_UPDATE_COUNT 1 NO_UPDATE_COUNT
useCachedCursor	boolean		JDBC driver property: useCachedCursor.
useIdentityValLocalForAutoGeneratedKeys	boolean		JDBC driver property: useIdentityValLocalForAutoGeneratedKeys.
useJDBC41DefinitionForGetColumns	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC41DefinitionForGetColumns. 2 NO 1 YES
useJDBC4ColumnNameAndLabelSemantics	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
useTransactionRedirect	boolean		JDBC driver property: useTransactionRedirect.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaNetworkOptimization	boolean		JDBC driver property: xaNetworkOptimization.

**dataSource > properties.derby.client**

Data source properties for Derby Network Client JDBC driver.

false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1527	Port on which to obtain database connections.
retrieveMessageText	boolean	true	JDBC driver property: retrieveMessageText.
securityMechanism	<ul style="list-style-type: none"> <li>3</li> <li>7</li> <li>4</li> <li>9</li> <li>8</li> </ul>	3	<p>JDBC driver property: securityMechanism. Values are:</p> <p>3 (CLEAR_TEXT_PASSWORD_SECURITY),</p> <p>4 (USER_ONLY_SECURITY),</p> <p>7 (ENCRYPTED_PASSWORD_SECURITY),</p> <p>8 (STRONG_PASSWORD_SUBSTITUTE_SECURITY),</p> <p>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY)</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY</p> <p>7 ENCRYPTED_PASSWORD_SECURITY</p> <p>4 USER_ONLY_SECURITY</p> <p>9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p> <p>8 STRONG_PASSWORD_SUBSTITUTE_SECURITY</p>

Attribute name	Data type	Default value	Description
serverName	string	localhost	Server where the database is running.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		JDBC driver property: shutdownDatabase. <b>false</b> Do not shut down the database. <b>shutdown</b> Shut down the database when a connection is attempted.
ssl	<ul style="list-style-type: none"> <li>basic</li> <li>off</li> <li>peerAuthentication</li> </ul>		JDBC driver property: ssl. <b>basic</b> basic <b>off</b> off <b>peerAuthentication</b> peerAuthentication
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_XA_CALLS=2048, TRACE_ALL=-1.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**dataSource > properties.derby.embedded**

Data source properties for Derby Embedded JDBC driver.

false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		<p>JDBC driver property: shutdownDatabase.</p> <p><b>false</b> Do not shut down the database.</p> <p><b>shutdown</b> Shut down the database when a connection is attempted.</p>
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

#### dataSource > properties.informix

Data source properties for the Informix JDBC driver.

false

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
ifxCLIENT_LOCALE	string		JDBC driver property: ifxCLIENT_LOCALE.
ifxCPMAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMInitPoolSize	int		JDBC driver property: ifxCPMInitPoolSize.
ifxCPMMaxConnections	int		JDBC driver property: ifxCPMMaxConnections.
ifxCPMMaxPoolSize	int		JDBC driver property: ifxCPMMaxPoolSize.
ifxCPMMinAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMMinAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMMinPoolSize	int		JDBC driver property: ifxCPMMinPoolSize.
ifxCPMServiceInterval	A period of time with millisecond precision		JDBC driver property: ifxCPMServiceInterval. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxDBANSIWARN	boolean		JDBC driver property: ifxDBANSIWARN.
ifxDBCENTURY	string		JDBC driver property: ifxDBCENTURY.
ifxDBDATE	string		JDBC driver property: ifxDBDATE.
ifxDBSPACETEMP	string		JDBC driver property: ifxDBSPACETEMP.

Attribute name	Data type	Default value	Description
ifxDBTEMP	string		JDBC driver property: ifxDBTEMP.
ifxDBTIME	string		JDBC driver property: ifxDBTIME.
ifxDBUPSPACE	string		JDBC driver property: ifxDBUPSPACE.
ifxDB_LOCALE	string		JDBC driver property: ifxDB_LOCALE.
ifxDELIMIDENT	boolean		JDBC driver property: ifxDELIMIDENT.
ifxENABLE_TYPE_CACHE	boolean		JDBC driver property: ifxENABLE_TYPE_CACHE.
ifxFET_BUF_SIZE	int		JDBC driver property: ifxFET_BUF_SIZE.
ifxGL_DATE	string		JDBC driver property: ifxGL_DATE.
ifxGL_DATETIME	string		JDBC driver property: ifxGL_DATETIME.
ifxIFXHOST	string	localhost	JDBC driver property: ifxIFXHOST.
ifxIFX_AUTOFREE	boolean		JDBC driver property: ifxIFX_AUTOFREE.
ifxIFX_DIRECTIVES	string		JDBC driver property: ifxIFX_DIRECTIVES.
ifxIFX_LOCK_MODE_WAIT	A period of time with second precision	2s	JDBC driver property: ifxIFX_LOCK_MODE_WAIT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxIFX_SOC_TIMEOUT	A period of time with millisecond precision		JDBC driver property: ifxIFX_SOC_TIMEOUT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxIFX_USEPUT	boolean		JDBC driver property: ifxIFX_USEPUT.

Attribute name	Data type	Default value	Description
ifxIFX_USE_STRENC	boolean		JDBC driver property: ifxIFX_USE_STRENC.
ifxIFX_XASPEC	string	y	JDBC driver property: ifxIFX_XASPEC.
ifxINFORMIXCONRETRY	int		JDBC driver property: ifxINFORMIXCONRETRY.
ifxINFORMIXCONTIME	A period of time with second precision		JDBC driver property: ifxINFORMIXCONTIME. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxINFORMIXOPCACHE	string		JDBC driver property: ifxINFORMIXOPCACHE.
ifxINFORMIXSTACKSIZE	int		JDBC driver property: ifxINFORMIXSTACKSIZE.
ifxJDBCTEMP	string		JDBC driver property: ifxJDBCTEMP.
ifxLDAP_IFXBASE	string		JDBC driver property: ifxLDAP_IFXBASE.
ifxLDAP_PASSWD	string		JDBC driver property: ifxLDAP_PASSWD.
ifxLDAP_URL	string		JDBC driver property: ifxLDAP_URL.
ifxLDAP_USER	string		JDBC driver property: ifxLDAP_USER.
ifxLOBCACHE	int		JDBC driver property: ifxLOBCACHE.
ifxNEWCODESET	string		JDBC driver property: ifxNEWCODESET.
ifxNEWLOCALE	string		JDBC driver property: ifxNEWLOCALE.
ifxNODEFDAC	string		JDBC driver property: ifxNODEFDAC.
ifxOPTCOMPIND	string		JDBC driver property: ifxOPTCOMPIND.
ifxOPTOFC	string		JDBC driver property: ifxOPTOFC.
ifxOPT_GOAL	string		JDBC driver property: ifxOPT_GOAL.
ifxPATH	string		JDBC driver property: ifxPATH.
ifxPDQPRIORITY	string		JDBC driver property: ifxPDQPRIORITY.

Attribute name	Data type	Default value	Description
ifxPLCONFIG	string		JDBC driver property: ifxPLCONFIG.
ifxPLOAD_LO_PATH	string		JDBC driver property: ifxPLOAD_LO_PATH.
ifxPROTOCOLTRACE	int		JDBC driver property: ifxPROTOCOLTRACE.
ifxPROTOCOLTRACEFILE	string		JDBC driver property: ifxPROTOCOLTRACEFILE.
ifxPROXY	string		JDBC driver property: ifxPROXY.
ifxPSORT_DBTEMP	string		JDBC driver property: ifxPSORT_DBTEMP.
ifxPSORT_NPROCS	boolean		JDBC driver property: ifxPSORT_NPROCS.
ifxSECURITY	string		JDBC driver property: ifxSECURITY.
ifxSQLH_FILE	string		JDBC driver property: ifxSQLH_FILE.
ifxSQLH_LOC	string		JDBC driver property: ifxSQLH_LOC.
ifxSQLH_TYPE	string		JDBC driver property: ifxSQLH_TYPE.
ifxSSLCONNECTION	string		JDBC driver property: ifxSSLCONNECTION.
ifxSTMT_CACHE	string		JDBC driver property: ifxSTMT_CACHE.
ifxTRACE	int		JDBC driver property: ifxTRACE.
ifxTRACEFILE	string		JDBC driver property: ifxTRACEFILE.
ifxTRUSTED_CONTEXT	string		JDBC driver property: ifxTRUSTED_CONTEXT.
ifxUSEV5SERVER	boolean		JDBC driver property: ifxUSEV5SERVER.
ifxUSE_DTENV	boolean		JDBC driver property: ifxUSE_DTENV.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
roleName	string		JDBC driver property: roleName.
serverName	string		Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**dataSource > properties.informix.jcc**

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for Informix.

false

Attribute name	Data type	Default value	Description
DBANSIWARN	boolean		JDBC driver property: DBANSIWARN.
DBDATE	string		JDBC driver property: DBDATE.
DBPATH	string		JDBC driver property: DBPATH.
DBSPACETEMP	string		JDBC driver property: DBSPACETEMP.
DBTEMP	string		JDBC driver property: DBTEMP.
DBUPSPACE	string		JDBC driver property: DBUPSPACE.
DELIMIDENT	boolean		JDBC driver property: DELIMIDENT.
IFX_DIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_DIRECTIVES. <b>ON</b> ON <b>OFF</b> OFF
IFX_EXTDIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_EXTDIRECTIVES. <b>ON</b> ON <b>OFF</b> OFF
IFX_UPDESC	string		JDBC driver property: IFX_UPDESC.

Attribute name	Data type	Default value	Description
IFX_XASTDCOMPLIANCE_XAEND	<ul style="list-style-type: none"> <li>0</li> </ul>		JDBC driver property: IFX_XASTDCOMPLIANCE_XAEND. <b>1</b> 1 <b>0</b> 0
INFORMIXOPCACHE	string		JDBC driver property: INFORMIXOPCACHE.
INFORMIXSTACKSIZE	string		JDBC driver property: INFORMIXSTACKSIZE.
NODEFDAC	<ul style="list-style-type: none"> <li>yes</li> <li>no</li> </ul>		JDBC driver property: NODEFDAC. <b>yes</b> yes <b>no</b> no
OPTCOMPIND	<ul style="list-style-type: none"> <li>2</li> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTCOMPIND. <b>2</b> 2 <b>1</b> 1 <b>0</b> 0
OPTOFC	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTOFC. <b>1</b> 1 <b>0</b> 0
PDQPRIORITY	<ul style="list-style-type: none"> <li>HIGH</li> <li>LOW</li> <li>OFF</li> </ul>		JDBC driver property: PDQPRIORITY. <b>HIGH</b> HIGH <b>LOW</b> LOW <b>OFF</b> OFF
PSORT_DBTEMP	string		JDBC driver property: PSORT_DBTEMP.
PSORT_NPROCS	string Maximum: 10		JDBC driver property: PSORT_NPROCS.
STMT_CACHE	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: STMT_CACHE. <b>1</b> 1 <b>0</b> 0
currentLockTimeout	A period of time with second precision	2s	JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean		JDBC driver property: deferPrepares.
driverType	int	4	JDBC driver property: driverType.
enableNamedParameterMarkers	int		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO).
enableSeamlessFailover	int		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO).
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.
keepDynamic	int		JDBC driver property: keepDynamic.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
progressiveStreaming	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		JDBC driver property: progressiveStreaming. Values are: 1 (YES) or 2 (NO).  2 NO 1 YES
queryDataSize	int Minimum: 4096 Maximum: 10485760		JDBC driver property: queryDataSize.

Attribute name	Data type	Default value	Description
resultSetHoldability	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
retrieveMessagesFromServerOnGetMessage	boolean	true	<p>JDBC driver property: retrieveMessagesFromServerOnGetMessage.</p>
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 9</li> </ul>		<p>JDBC driver property: securityMechanism. Values are: 3 (CLEAR_TEXT_PASSWORD_SECURITY), 4 (USER_ONLY_SECURITY), 7 (ENCRYPTED_PASSWORD_SECURITY), 9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY).</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY 7 ENCRYPTED_PASSWORD_SECURITY 4 USER_ONLY_SECURITY 9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p>
serverName	string	localhost	Server where the database is running.
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.

Attribute name	Data type	Default value	Description
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
useJDBC4ColumnNameAndLabelSemantics	int		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO).
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

#### dataSource > properties.microsoft.sqlserver

Data source properties for Microsoft SQL Server JDBC Driver.

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database. Example: jdbc:sqlserver://localhost:1433;databaseName=myDB.
applicationIntent	<ul style="list-style-type: none"> <li>ReadOnly</li> <li>ReadWrite</li> </ul>		JDBC driver property: applicationIntent. <b>ReadOnly</b> ReadOnly <b>ReadWrite</b> ReadWrite
applicationName	string		JDBC driver property: applicationName.
authenticationScheme	<ul style="list-style-type: none"> <li>NativeAuthentication</li> <li>JavaKerberos</li> </ul>		JDBC driver property: authenticationScheme. <b>NativeAuthentication</b> NativeAuthentication <b>JavaKerberos</b> JavaKerberos

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
encrypt	boolean		JDBC driver property: encrypt.
failoverPartner	string		JDBC driver property: failoverPartner.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
instanceName	string		JDBC driver property: instanceName.
integratedSecurity	boolean		JDBC driver property: integratedSecurity.
lastUpdateCount	boolean		JDBC driver property: lastUpdateCount.
lockTimeout	A period of time with millisecond precision		JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
multiSubnetFailover	boolean		JDBC driver property: multiSubnetFailover.
packetSize	int Minimum: 512 Maximum: 32767		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.

Attribute name	Data type	Default value	Description
responseBuffering	<ul style="list-style-type: none"> <li>full</li> <li>adaptive</li> </ul>		JDBC driver property: responseBuffering. <b>full</b> full <b>adaptive</b> adaptive
selectMethod	<ul style="list-style-type: none"> <li>direct</li> <li>cursor</li> </ul>		JDBC driver property: selectMethod. <b>direct</b> direct <b>cursor</b> cursor
sendStringParametersAsUnicode	boolean	false	JDBC driver property: sendStringParametersAsUnicode.
sendTimeAsDatetime	boolean		JDBC driver property: sendTimeAsDatetime.
serverName	string	localhost	Server where the database is running.
trustServerCertificate	boolean		JDBC driver property: trustServerCertificate.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
workstationID	string		JDBC driver property: workstationID.
xopenStates	boolean		JDBC driver property: xopenStates.

#### dataSource > properties.oracle

Data source properties for Oracle JDBC driver.

false

Attribute name	Data type	Default value	Description
ONSConfiguration	string		JDBC driver property: ONSConfiguration.
TNSEntryName	string		JDBC driver property: TNSEntryName.
URL	string		URL for connecting to the database. Examples: jdbc:oracle:thin://localhost:1521/sample or jdbc:oracle:oci://localhost:1521/sample.
connectionProperties	string		JDBC driver property: connectionProperties.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
driverType	<ul style="list-style-type: none"> <li>oci</li> <li>thin</li> </ul>	thin	JDBC driver property: driverType.  <b>oci</b> oci <b>thin</b> thin
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	string		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1521	Port on which to obtain database connections.
serverName	string	localhost	Server where the database is running.
serviceName	string		JDBC driver property: serviceName.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

#### dataSource > properties.sybase

Data source properties for Sybase JDBC driver.

false

Attribute name	Data type	Default value	Description
SERVER_INITIATED_TRANSACTIONS	<ul style="list-style-type: none"> <li>false</li> <li>true</li> </ul>	false	JDBC driver property: SERVER_INITIATED_TRANSACTIONS.  <b>false</b> false <b>true</b> true
connectionProperties	string	SELECT_OPENS_CURSOR=true	JDBC driver property: connectionProperties.
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	<ul style="list-style-type: none"> <li>• SSL</li> <li>• socket</li> </ul>		JDBC driver property: networkProtocol.  <b>SSL</b> SSL <b>socket</b> socket
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	5000	Port on which to obtain database connections.
resourceManagerName	string		JDBC driver property: resourceManagerName.
serverName	string	localhost	Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
version	int		JDBC driver property: version.

**dataSource > recoveryAuthData**

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## DeployManager (deployManager)

DeployManager

Attribute name	Data type	Default value	Description
maxResults	int	100	The maximum number of deploy results to hold in memory. After the maximum is reached, the oldest result is discarded.

## Deploy Rule (deployRule)

The rule used to deploy a member

- inputVariable
- runtimeTpe

Attribute name	Data type	Default value	Description
deploy	string		The command to deploy a member
id	string		A unique configuration ID.
name	string		The name of the deploy rule
restart	string		The command to restart a deployed member
start	string		The command to start a deployed member
stop	string		The command to stop a deployed member
type	string		The type of member to be deployed
undeploy	string		The command to undeploy a member

### inputVariable

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
defaultValue	string		The default value for the input variable
description	string		The description of the input variable
displayName	string		The display name of the input variable
group	string		The group of the input variable
id	string		A unique configuration ID.
name	string		The name of the input variable

Attribute name	Data type	Default value	Description
type	string		The type of the input variable

### runtimeTpe

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
displayName	string		The display name for the runtime
id	string		A unique configuration ID.

## DeployVariable (deployVariable)

The deploy variable configuration element.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
increment	int	0	Increment value for the deployVariable.
name	string		Name for the deployVariable.
value	string		Initial value of the deployVariable.

## Distributed Map (distributedMap)

Distributed map configuration for a local cache.

- cacheGroup
  - member
    - adapterBeanName
- diskCache
- library
  - file
  - fileset
  - folder

Attribute name	Data type	Default value	Description
cacheProviderName	string	default	Specifies the name of an alternate cache provider.
highThreshold	int Minimum: -1 Maximum: 100	-1	Specifies when the memory cache eviction policy starts. The threshold is expressed in terms of the percentage of the memory cache size in megabytes (MB).
id	string		A unique configuration ID.
jndiName	string	\${id}	JNDI name for a cache instance.

Attribute name	Data type	Default value	Description
libraryRef	A reference to top level library element (string).		Specifies a reference to a shared library.
lowThreshold	int Minimum: -1 Maximum: 100	-1	Specifies when the memory cache eviction policy ends. The threshold is expressed in terms of the percentage of the memory cache size in megabytes (MB).
memorySizeInEntries	int Minimum: 0	2000	Specifies a positive integer that defines the maximum number of entries that the cache can hold. Values are usually in the thousands. The minimum value is 100, with no set maximum value. The default value is 2000.
memorySizeInMB	int Minimum: -1	-1	Specifies a value for the maximum memory cache size in megabytes (MB).

#### cacheGroup

Specifies sets of external caches that are controlled by WebSphere(R) Application Server on servers such as IBM(R) WebSphere(R) Edge Server and IBM(R) HTTP Server.

false

Attribute name	Data type	Default value	Description
name	string		Specifies a unique name for the external cache group. The external cache group name must match the ExternalCache property that is defined in the servlet or Java(TM) Server Pages (JSP) cachespec.xml file.

#### cacheGroup > member

Members of an external cache group that are controlled by WebSphere Application Server.

false

Attribute name	Data type	Default value	Description
host	string		Fully qualified host name
port	int Minimum: 0		Port.

#### cacheGroup > member > adapterBeanName

Specifies the name of a class, which is located on the WebSphere Application Server class path, of the adapter between WebSphere Application Server and this external cache.

false

string

## diskCache

Enable disk offload to specify that when the cache is full, cache entries are removed from the cache and saved to disk. The location is a fully-qualified directory location that is used by the disk offload function. The Flush to Disk on Stop option specifies that when the server stops, the contents of the memory cache are moved to disk.

false

Attribute name	Data type	Default value	Description
evictionPolicy	<ul style="list-style-type: none"><li>• RANDOM</li><li>• SIZE</li></ul>	RANDOM	Specifies the eviction algorithm and thresholds that the disk cache uses to evict entries. When the disk size reaches a high threshold limit, the disk cache garbage collector wakes up and evicts randomly-selected (Random) or the largest (Size) entries on the disk until the disk size reaches a low threshold limit. <b>RANDOM</b> Random <b>SIZE</b> Size
flushToDiskOnStopEnabled	boolean	false	Set this value to true to have objects that are cached in memory saved to disk when the server stops. This value is ignored if Enable disk offload is set to false.
highThreshold	int Minimum: 0 Maximum: 100	80	Specifies when the eviction policy starts.
location	Path to a directory		Specifies a directory to use for disk offload.
lowThreshold	int Minimum: 0 Maximum: 100	70	Specifies when the eviction policy ends.
sizeInEntries	int Minimum: 0	100000	Specifies a value for the maximum disk cache size, in number of entries.
sizeInGB	int Minimum: 3	3	Specifies a value for the maximum disk cache size, in gigabytes (GB).

## library

Specifies a reference to a shared library.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

### library > file

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

### library > fileset

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

### library > folder

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

## SIP Domain Resolver (domainResolver)

Configuration for the SIP domain resolver

- dnsServers

Attribute name	Data type	Default value	Description				
addTtl	boolean	false	Add an IBMTTL parameter to the SIP URI.				
dnsAllowedFailures	int	5	The number of allowed DNS lookup failures for the DNS failover mechanism.				
dnsAutoResolve	boolean	false	Resolve domain names automatically.				
dnsEdns	<ul style="list-style-type: none"> <li>• N</li> <li>• Y</li> </ul>	Y	Defines the transport protocol for DNS lookup to resolve RFC 3263 SIP URIs. If set to Y, UDP is used. If set to N, TCP is used. <table border="0" style="margin-left: 20px;"> <tr> <td>N</td> <td>N</td> </tr> <tr> <td>Y</td> <td>Y</td> </tr> </table>	N	N	Y	Y
N	N						
Y	Y						

Attribute name	Data type	Default value	Description
dnsRequestCacheTimeoutMin	A period of time with minute precision	10m	The minimum time in minutes after which cached DNS queries time out. Specify a positive integer followed by a unit of time, which can be hours (h) or minutes (m). For example, specify 30 minutes as 30m. You can include multiple values in a single entry. For example, 1h30m is equivalent to 90 minutes.
dnsSingleQueryTimeoutSec	A period of time with second precision	5s	The number of seconds after which a single query times out for the DNS failover mechanism. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
dnsUdpPayloadSize	short Minimum: 512 Maximum: 32767	1280	The UDP payload size in bytes for the DNS resolver service.
dnsWindowSizeInterval	int	10	The resolver service window size interval for the DNS failover mechanism.
dnsWindowSizeMin	int	600	The minimum window size for the DNS failover mechanism.

### dnsServers

Allows a SIP URI to be resolved through DNS into the IP address, port, and transport protocol. The value is a String that contains exactly one or two address and port tuples, where two tuples are separated by a space.

false

string

## IBM Lotus Domino LDAP Filters (domino50LdapFilterProperties)

Specifies the list of default IBM Lotus Domino LDAP filters.

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(objectclass=dominoGroup))	An LDAP filter clause for searching the user registry for groups.

Attribute name	Data type	Default value	Description
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	dominoGroup:member	An LDAP filter that identifies user to group memberships.
id	string		A unique configuration ID.
userFilter	string	(&(uid=%v)(objectclass=Person))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	person:uid	An LDAP filter that maps the name of a user to an LDAP entry.

## Dynamic Routing (dynamicRouting)

Defines Dynamic Routing specific configuration options.

- pluginProperty
- routingRules
  - routingRule
    - permitAction
      - loadBalanceEndPoints
        - endPoint
    - redirectAction
    - rejectAction
- traceSpecification

Attribute name	Data type	Default value	Description
connectorClusterName	string		The name of the connector cluster.
maxRetries	int Minimum: -1	-1	The maximum number of retry attempts. Specifying -1 (default) disables the limit.
retryInterval	A period of time with second precision	60s	The retry interval duration. The default value is 60 seconds. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

### pluginProperty

A custom property for the WebSphere plug-in configuration. This property is directly inserted into the generated WebSphere plug-in configuration file.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		The name of the custom property. This name is directly inserted into the generated WebSphere plug-in configuration file.
scope	<ul style="list-style-type: none"> <li>connectorCluster</li> <li>intelligentManagement</li> </ul>	intelligentManagement	<p>The scope of the custom property. This determines which generated WebSphere plug-in configuration file stanza it is nested upon.</p> <p><b>connectorCluster</b> ConnectorCluster</p> <p><b>intelligentManagement</b> IntelligentManagement</p>
value	string		The value of the custom property. This value is directly inserted into the generated WebSphere plug-in configuration file.

### routingRules

Set of routing rules

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
webServers	string	*	Web servers for which the routing rules have to be created.

### routingRules > routingRule

Routing rule as part of the routing rule set

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchExpression	string	false	Expression to be matched
order	string		Order

### routingRules > routingRule > permitAction

Permit action

false

Attribute name	Data type	Default value	Description
allowMaintenanceModeServers	boolean	false	Check it to permit requests to maintenance mode servers

**routingRules > routingRule > permitAction > loadBalanceEndpoints**

Destination end points between which the requests have to be load balanced

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

**routingRules > routingRule > permitAction > loadBalanceEndpoints > endPoint**

Target destination for the routing rule

false

Attribute name	Data type	Default value	Description
destination	string	*	Destination
id	string		A unique configuration ID.

**routingRules > routingRule > redirectAction**

Redirect action

false

Attribute name	Data type	Default value	Description
redirectAction.location	string		URL to which the redirect should be done

**routingRules > routingRule > rejectAction**

Reject action

false

Attribute name	Data type	Default value	Description
rejectAction.code	string	404	The status code to be returned on reject

**traceSpecification**

A custom trace specification for the WebSphere plug-in configuration. This property is directly inserted into the generated WebSphere plug-in configuration file.

false

Attribute name	Data type	Default value	Description
condition	string		When a request satisfies this condition, specified trace specification will be enabled for the request. This value should not be left blank for non-default specifications. It is directly inserted into the generated WebSphere plug-in configuration file.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
name	string		The name of the trace specification property. Trace specifications for the same webserver should have unique names. Only the most specific, latest specification with the same name is inserted into the generated WebSphere plug-in configuration file.
specification	string		The value of the trace specification property. This value is directly inserted into the generated WebSphere plug-in configuration file.
webservers	string	*	Webservers for which the trace specification applies. Comma-separated list of webserver names for which the specification should be inserted into the generated WebSphere plug-in configuration file. Specify "*" (default) for all webservers.

## Novell eDirectory LDAP Filters (edirectoryLdapFilterProperties)

Specifies the list of Novell eDirectory LDAP filters.

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(objectclass=groupOfNames))	An LDAP filter clause for searching the user registry for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	groupOfNames:member	An LDAP filter that identifies user to group memberships.
id	string		A unique configuration ID.
userFilter	string	(&(cn=%v)(objectclass=Person))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	person:cn	An LDAP filter that maps the name of a user to an LDAP entry.

## EJB Application (ejbApplication)

Defines the properties of an EJB application.

- application-bnd

- security-role
  - group
  - run-as
  - special-subject
  - user
- classloader
  - commonLibrary
    - file
    - fileset
    - folder
  - privateLibrary
    - file
    - fileset
    - folder

Attribute name	Data type	Default value	Description
autoStart	boolean	true	Indicates whether or not the server automatically starts the application.
context-root	string		Context root of an application.
id	string		A unique configuration ID.
location	A file, directory or url.		Location of an application expressed as an absolute path or a path relative to the server-level apps directory.
name	string		Name of an application.
suppressUncoveredHttpMethodWarning	boolean	false	Option to suppress uncovered HTTP method warning message during application deployment.

### application-bnd

Binds general deployment information included in the application to specific resources.

false

Attribute name	Data type	Default value	Description
version	string		Version of the application bindings specification.

### application-bnd > security-role

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Name of a security role.

**application-bnd > security-role > group**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		Group access ID
id	string		A unique configuration ID.
name	string		Name of a group possessing a security role.

**application-bnd > security-role > run-as**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
password	Reversably encoded password (string)		Password of a user required to access a bean from another bean. The value can be stored in clear text or encoded form. To encode the password, use the securityUtility tool with the encode option.
userid	string		ID of a user required to access a bean from another bean.

**application-bnd > security-role > special-subject**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
type	<ul style="list-style-type: none"> <li>• EVERYONE</li> <li>• ALL_AUTHENTICATED_USERS</li> </ul>		One of the following special subject types: ALL_AUTHENTICATED_USERS, EVERYONE.  <b>EVERYONE</b> Everyone  <b>ALL_AUTHENTICATED_USERS</b> All authenticated users

**application-bnd > security-role > user**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		A user access ID in the general form user:realmName/userUniqueId. A value will be generated if one is not specified.
id	string		A unique configuration ID.
name	string		Name of a user possessing a security role.

### classloader

Defines the settings for an application classloader.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
classProviderRef	List of references to top level resourceAdapter elements (comma-separated string).		List of class provider references. When searching for classes or resources, this class loader will delegate to the specified class providers after searching its own class path.
commonLibraryRef	List of references to top level library elements (comma-separated string).		List of library references. Library class instances are shared with other classloaders.
delegation	<ul style="list-style-type: none"> <li>parentFirst</li> <li>parentLast</li> </ul>	parentFirst	Controls whether parent classloader is used before or after this classloader. If parent first is selected then delegate to immediate parent before searching the classpath. If parent last is selected then search the classpath before delegating to the immediate parent.  <b>parentFirst</b> Parent first  <b>parentLast</b> Parent last
privateLibraryRef	List of references to top level library elements (comma-separated string).		List of library references. Library class instances are unique to this classloader, independent of class instances from other classloaders.

**classloader > commonLibrary**

List of library references. Library class instances are shared with other classloaders.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
id	string		A unique configuration ID.
name	string		Name of shared library for administrators

**classloader > commonLibrary > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**classloader > commonLibrary > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**classloader > commonLibrary > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**classloader > privateLibrary**

List of library references. Library class instances are unique to this classloader, independent of class instances from other classloaders.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
id	string		A unique configuration ID.
name	string		Name of shared library for administrators

**classloader > privateLibrary > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**classloader > privateLibrary > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**classloader > privateLibrary > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

## EJB Container (ejbContainer)

Defines the behavior of the EJB container.

- asynchronous
  - contextService
    - baseContext
      - baseContext
      - classloaderContext
      - jeeMetadataContext
      - securityContext
      - syncToOSThreadContext
      - zosWLMContext
    - classloaderContext
    - jeeMetadataContext
    - securityContext
    - syncToOSThreadContext
    - zosWLMContext
- timerService
  - persistentExecutor
    - contextService
      - baseContext
        - baseContext
        - classloaderContext
        - jeeMetadataContext
        - securityContext
        - syncToOSThreadContext
        - zosWLMContext
      - classloaderContext
      - jeeMetadataContext
      - securityContext
      - syncToOSThreadContext
      - zosWLMContext

Attribute name	Data type	Default value	Description
cacheCleanupInterval	A period of time with second precision	3s	The interval between passivating unused stateful session bean instances when the size is exceeded. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
cacheSize	int Minimum: 1	2053	The number of stateful session bean instances that should be cached in memory.
poolCleanupInterval	A period of time with second precision	30s	The interval between removing unused bean instances. This setting only applies to stateless session and message-driven beans. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
startEJBsAtAppStart	boolean		Specifies when EJB types will be initialized. If this property is set to true, EJB types will be initialized at the time applications are first started. If this property is set to false, EJB types will be initialized at the time the EJB type is first used by an application. If this property is not set, the behavior is determined on a bean-by-bean basis from the start-at-app-start attribute in the ibm-ejb-jar-ext.xml file. This setting does not apply to either message-driven or startup singleton beans. Message-driven and startup singleton beans will always be initialized at the time applications are started.

**asynchronous**

Defines the behavior of EJB asynchronous methods.

false

Attribute name	Data type	Default value	Description
contextServiceRef	A reference to top level contextService element (string).		The context service used to manage context propagation to asynchronous EJB method threads.
maxUnclaimedRemoteResults	sint Minimum: 1	1000	The maximum number of unclaimed results that the server retains from all remote asynchronous method calls that return a Future object. If the maximum is exceeded, the server purges the result of the method call that completed the longest ago to prevent memory leakage.
unclaimedRemoteResultTimeout	A period of time with second precision	24h	The amount of time that the server retains the result for each remote asynchronous method call that returns a Future object. If an application does not claim the result within the specified period of time, the server purges the result of that method call to prevent memory leakage. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**asynchronous > contextService**

The context service used to manage context propagation to asynchronous EJB method threads.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**asynchronous > contextService > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
id	string		A unique configuration ID.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**asynchronous > contextService > baseContext > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

com.ibm.ws.context.service-factory

**asynchronous > contextService > baseContext > classloaderContext**

Classloader context propagation configuration.

false

**asynchronous > contextService > baseContext > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**asynchronous > contextService > baseContext > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**asynchronous > contextService > baseContext > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**asynchronous > contextService > baseContext > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"><li>• Propagate</li><li>• PropagateOrNew</li><li>• New</li></ul>	Propagate	Indicates how the WLM context should be handled for non-Daemon work. <b>Propagate</b> Use the same WLM Context (if one exists). <b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists. <b>New</b> Always create a new WLM context.

**asynchronous > contextService > classloaderContext**

Classloader context propagation configuration.

false

**asynchronous > contextService > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**asynchronous > contextService > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**asynchronous > contextService > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**asynchronous > contextService > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"> <li>• Propagate</li> <li>• PropagateOrNew</li> <li>• New</li> </ul>	Propagate	<p>Indicates how the WLM context should be handled for non-Daemon work.</p> <p><b>Propagate</b> Use the same WLM Context (if one exists).</p> <p><b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists.</p> <p><b>New</b> Always create a new WLM context.</p>

**timerService**

Defines the behavior of the EJB timer service.

false

Attribute name	Data type	Default value	Description
lateTimerThreshold	A period of time with minute precision	5m	Number of minutes after the scheduled expiration of a timer that the start of the timer will be considered late. When a timer does start late, a warning message will be logged indicating that the timer has started later than scheduled. The default threshold is 5 minutes and a value of 0 minutes turns off the warning message feature. Specify a positive integer followed by a unit of time, which can be hours (h) or minutes (m). For example, specify 30 minutes as 30m. You can include multiple values in a single entry. For example, 1h30m is equivalent to 90 minutes.
nonPersistentMaxRetries	int Minimum: -1	-1	When a non-persistent timer expires, the timeout callback method is called. This setting controls how many times the EJB container attempts to retry the timer. If the transaction for this callback method fails or is rolled back, the EJB container must retry the timer at least once. The default value is -1, which means the EJB container retries infinitely until the timer is successful. If the value is set to 0, the EJB container does not retry the timer, however, this results in behavior that is not compliant with the EJB specification.

Attribute name	Data type	Default value	Description
nonPersistentRetryInterval	A period of time with second precision	300s	When a non-persistent timer expires, the timeout callback method is called. If the transaction for this callback method fails or is rolled back, the container must retry the timer. The first retry attempt occurs immediately, and subsequent retry attempts are delayed by the number of seconds specified. If the value is set to 0, then all retries occur immediately. If you do not specify a value, the default interval is 300 seconds. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
persistentExecutorRef	A reference to top level persistentExecutor element (string).		Schedules and runs EJB persistent timer tasks.

**timerService > persistentExecutor**

Schedules and runs EJB persistent timer tasks.

false

Attribute name	Data type	Default value	Description
contextServiceRef	A reference to top level contextService element (string).	DefaultContextService	Configures how context is captured and propagated to threads.
enableTaskExecution	boolean	true	Determines whether or not this instance may run tasks.

Attribute name	Data type	Default value	Description
initialPollDelay	A period of time with millisecond precision	0	Duration of time to wait before this instance might poll the persistent store for tasks to run. A value of -1 delays polling until it is started programmatically. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
pollInterval	A period of time with millisecond precision	-1	Interval between polling for tasks to run. A value of -1 disables all polling after the initial poll. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
pollSize	int Minimum: 1		The maximum number of task entries to find when polling the persistent store for tasks to run. If unspecified, there is no limit.
retryInterval	A period of time with millisecond precision	1m	The amount of time that must pass between the second and subsequent consecutive retries of a failed task. The first retry occurs immediately, regardless of the value of this attribute. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
retryLimit	short Minimum: -1 Maximum: 10000	10	Limit of consecutive retries for a task that has failed or rolled back, after which the task is considered permanently failed and does not attempt further retries. A value of -1 allows for unlimited retries.
taskStoreRef	A reference to top level databaseStore element (string).	defaultDatabaseStore	Persistent store for scheduled tasks.

**timerService > persistentExecutor > contextService**

Configures how context is captured and propagated to threads.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**timerService > persistentExecutor > contextService > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
id	string		A unique configuration ID.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**timerService > persistentExecutor > contextService > baseContext > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

com.ibm.ws.context.service-factory

**timerService > persistentExecutor > contextService > baseContext > classloaderContext**

Classloader context propagation configuration.

false

**timerService > persistentExecutor > contextService > baseContext > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**timerService > persistentExecutor > contextService > baseContext > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**timerService > persistentExecutor > contextService > baseContext > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**timerService > persistentExecutor > contextService > baseContext > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"><li>• Propagate</li><li>• PropagateOrNew</li><li>• New</li></ul>	Propagate	Indicates how the WLM context should be handled for non-Daemon work. <b>Propagate</b> Use the same WLM Context (if one exists). <b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists. <b>New</b> Always create a new WLM context.

**timerService > persistentExecutor > contextService > classloaderContext**

Classloader context propagation configuration.

false

**timerService > persistentExecutor > contextService > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**timerService > persistentExecutor > contextService > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**timerService > persistentExecutor > contextService > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**timerService > persistentExecutor > contextService > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"><li>• Propagate</li><li>• PropagateOrNew</li><li>• New</li></ul>	Propagate	Indicates how the WLM context should be handled for non-Daemon work. <b>Propagate</b> Use the same WLM Context (if one exists). <b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists. <b>New</b> Always create a new WLM context.

## Enterprise Application (enterpriseApplication)

Defines the properties of an enterprise application.

- application-bnd
  - security-role
    - group
    - run-as
    - special-subject
    - user
- classloader
  - commonLibrary
  - file
  - fileset
  - folder
  - privateLibrary

- file
- fileset
- folder
- resourceAdapter
  - contextService
    - baseContext
      - baseContext
      - classloaderContext
      - jeeMetadataContext
      - securityContext
      - syncToOSThreadContext
      - zosWLMContext
    - classloaderContext
    - jeeMetadataContext
    - securityContext
    - syncToOSThreadContext
    - zosWLMContext
  - customize

Attribute name	Data type	Default value	Description
autoStart	boolean	true	Indicates whether or not the server automatically starts the application.
defaultClientModule	string		Default client module of an enterprise application.
id	string		A unique configuration ID.
location	A file, directory or url.		Location of an application expressed as an absolute path or a path relative to the server-level apps directory.
name	string		Name of an application.
suppressUncoveredHttpMethodWarning	boolean	false	Option to suppress uncovered HTTP method warning message during application deployment.

### application-bnd

Binds general deployment information included in the application to specific resources.

false

Attribute name	Data type	Default value	Description
version	string		Version of the application bindings specification.

### application-bnd > security-role

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Name of a security role.

**application-bnd > security-role > group**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		Group access ID
id	string		A unique configuration ID.
name	string		Name of a group possessing a security role.

**application-bnd > security-role > run-as**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
password	Reversably encoded password (string)		Password of a user required to access a bean from another bean. The value can be stored in clear text or encoded form. To encode the password, use the securityUtility tool with the encode option.
userid	string		ID of a user required to access a bean from another bean.

**application-bnd > security-role > special-subject**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
type	<ul style="list-style-type: none"> <li>• EVERYONE</li> <li>• ALL_AUTHENTICATED_USERS</li> </ul>		One of the following special subject types: ALL_AUTHENTICATED_USERS, EVERYONE.  <b>EVERYONE</b> Everyone  <b>ALL_AUTHENTICATED_USERS</b> All authenticated users

**application-bnd > security-role > user**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		A user access ID in the general form user:realmName/userUniqueId. A value will be generated if one is not specified.
id	string		A unique configuration ID.
name	string		Name of a user possessing a security role.

### classloader

Defines the settings for an application classloader.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
classProviderRef	List of references to top level resourceAdapter elements (comma-separated string).		List of class provider references. When searching for classes or resources, this class loader will delegate to the specified class providers after searching its own class path.
commonLibraryRef	List of references to top level library elements (comma-separated string).		List of library references. Library class instances are shared with other classloaders.
delegation	<ul style="list-style-type: none"><li>parentFirst</li><li>parentLast</li></ul>	parentFirst	Controls whether parent classloader is used before or after this classloader. If parent first is selected then delegate to immediate parent before searching the classpath. If parent last is selected then search the classpath before delegating to the immediate parent. <b>parentFirst</b> Parent first <b>parentLast</b> Parent last

Attribute name	Data type	Default value	Description
privateLibraryRef	List of references to top level library elements (comma-separated string).		List of library references. Library class instances are unique to this classloader, independent of class instances from other classloaders.

**classloader > commonLibrary**

List of library references. Library class instances are shared with other classloaders.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
id	string		A unique configuration ID.
name	string		Name of shared library for administrators

**classloader > commonLibrary > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**classloader > commonLibrary > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.

Attribute name	Data type	Default value	Description
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**classloader > commonLibrary > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**classloader > privateLibrary**

List of library references. Library class instances are unique to this classloader, independent of class instances from other classloaders.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
id	string		A unique configuration ID.
name	string		Name of shared library for administrators

**classloader > privateLibrary > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**classloader > privateLibrary > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**classloader > privateLibrary > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**resourceAdapter**

Specifies configuration for a resource adapter that is embedded in an application.

false

Attribute name	Data type	Default value	Description
alias	string	#{id}	Overrides the default identifier for the resource adapter. The identifier is used in the name of the resource adapter's configuration properties element, which in turn is used in determining the name of configuration properties elements for any resources provided by the resource adapter. The resource adapter's configuration properties element name has the format, properties.<APP_NAME>.<ALIAS>, where <APP_NAME> is the name of the application and <ALIAS> is the configured alias. If unspecified, the alias defaults to the module name of the resource adapter.
autoStart	boolean		Configures whether a resource adapter starts automatically upon deployment of the resource adapter or lazily upon injection or lookup of a resource.
contextServiceRef	A reference to top level contextService element (string).		Configures how context is captured and propagated to threads.
id	string		Identifies the name of the embedded resource adapter module to which this configuration applies.

**resourceAdapter > contextService**

Configures how context is captured and propagated to threads.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**resourceAdapter > contextService > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
id	string		A unique configuration ID.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**resourceAdapter > contextService > baseContext > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

com.ibm.ws.context.service-factory

**resourceAdapter > contextService > baseContext > classloaderContext**

Classloader context propagation configuration.

false

**resourceAdapter > contextService > baseContext > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**resourceAdapter > contextService > baseContext > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**resourceAdapter > contextService > baseContext > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**resourceAdapter > contextService > baseContext > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"><li>• Propagate</li><li>• PropagateOrNew</li><li>• New</li></ul>	Propagate	Indicates how the WLM context should be handled for non-Daemon work. <b>Propagate</b> Use the same WLM Context (if one exists). <b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists. <b>New</b> Always create a new WLM context.

**resourceAdapter > contextService > classloaderContext**

Classloader context propagation configuration.

false

**resourceAdapter > contextService > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**resourceAdapter > contextService > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**resourceAdapter > contextService > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**resourceAdapter > contextService > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"> <li>• Propagate</li> <li>• PropagateOrNew</li> <li>• New</li> </ul>	Propagate	<p>Indicates how the WLM context should be handled for non-Daemon work.</p> <p><b>Propagate</b> Use the same WLM Context (if one exists).</p> <p><b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists.</p> <p><b>New</b> Always create a new WLM context.</p>

**resourceAdapter > customize**

Customizes the configuration properties element for the activation specification, administered object, or connection factory with the specified interface and/or implementation class.

false

Attribute name	Data type	Default value	Description
implementation	string		Fully qualified implementation class name for which the configuration properties element should be customized.
interface	string		Fully qualified interface class name for which the configuration properties element should be customized.

Attribute name	Data type	Default value	Description
suffix	string		Overrides the default suffix for the configuration properties element. For example, "CustomConnectionFactory" in properties.rarModule1.CustomConnectionFa The suffix is useful to disambiguate when multiple types of connection factories, administered objects, or endpoint activations are provided by a resource adapter. If a configuration properties element customization omits the suffix or leaves it blank, no suffix is used.

## Event Logging (eventLogging)

Logs a record of events, such as the JDBC requests and servlet requests, and their durations.

Attribute name	Data type	Default value	Description
eventTypes	string	all	A list of comma-separated event types that needs to be logged. Use all, to log all event types.
includeContextInfo	boolean	true	Indicates if the context information details are included in the log output.
logMode	<ul style="list-style-type: none"> <li>• entry</li> <li>• entryExit</li> <li>• exit</li> </ul>	exit	Controls whether the event logging occurs at the entry to events, at the exit from events, or both.  <b>entry</b> log at entry  <b>entryExit</b> log at entry and exit  <b>exit</b> log at exit
minDuration	A period of time with millisecond precision	1s	Exit entries will be logged for events longer than minDuration. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
sampleRate	int Minimum: 1	1	To sample one out of every n requests, set sampleRate to n. To sample all requests, set sampleRate to 1.

## Executor Management (executor)

Defines settings for the Liberty kernel default executor. Note that there is always one and exactly one default executor, for use by the Liberty runtime only and not directly accessible by applications.

Applications that need to configure and utilize executors should instead use Managed Executors.

Attribute name	Data type	Default value	Description
coreThreads	int	-1	Steady-state or core number of threads to associate with the executor. The number of threads associated with the executor will quickly grow to this number. If this value is less than 0, a default value is used. This default value is calculated based on the number of hardware threads on the system.
keepAlive	A period of time with millisecond precision	60s	Amount of time to keep an idle thread in the pool before allowing it to terminate. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
maxThreads	int	-1	Maximum number of threads that can be associated with the executor. If greater than 0, this value must be greater than or equal to the value of coreThreads. If the value of maxThreads is less than or equal to 0, the maximum number of threads is unbounded. Note that the actual number of threads associated with the executor is determined dynamically by the Liberty kernel, so leaving the maximum threads unbounded does not imply that the runtime will actively create large amounts of threads; it simply lets the Liberty kernel decide how many threads to associate with the executor without having a defined upper boundary.
name	string	Default Executor	The name of the Liberty kernel default executor.
rejectedWorkPolicy	<ul style="list-style-type: none"> <li>• CALLER_RUNS</li> <li>• ABORT</li> </ul>	ABORT	<p>Policy to employ when the executor is unable to stage work for execution.</p> <p><b>CALLER_RUNS</b> Execute the work immediately on the caller's thread.</p> <p><b>ABORT</b> Raise an exception.</p>

Attribute name	Data type	Default value	Description
stealPolicy	<ul style="list-style-type: none"> <li>• STRICT</li> <li>• NEVER</li> <li>• LOCAL</li> </ul>	LOCAL	<p>The work-stealing policy to employ. The options for this policy determine how work is queued, and how threads obtain queued work.</p> <p><b>STRICT</b> All threads that generate work own a local work pile. Threads that are associated with the executor take work from other threads when the local work pile is exhausted.</p> <p><b>NEVER</b> A global work queue is used to feed work to threads that are associated with the executor. No stealing will occur.</p> <p><b>LOCAL</b> A global work queue is used for work that is generated by threads that are not associated with the executor. Work generated by threads associated with the executor is placed on a local work pile. This work pile is owned by the generating thread, unless another thread steals it. Threads that are associated with the executor take work associated with other threads if the local work pile is empty and there is no work on the global work queue.</p>

## Feature Manager (featureManager)

Defines how the server loads features.

- feature

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"><li>• IGNORE</li><li>• FAIL</li><li>• WARN</li></ul>	WARN	Action to take after a failure to load a feature.  <b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.  <b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.  <b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.

### feature

Specifies a feature to be used when the server runs.

false

string

## User Registry Federation (federatedRepository)

Configuration for the user registry federation.

- extendedProperty
- primaryRealm
  - defaultParents
  - groupDisplayNameMapping
  - groupSecurityNameMapping
  - participatingBaseEntry
  - uniqueGroupIdMapping
  - uniqueUserIdMapping
  - userDisplayNameMapping
  - userSecurityNameMapping
- realm
  - defaultParents
  - groupDisplayNameMapping
  - groupSecurityNameMapping
  - participatingBaseEntry

- uniqueGroupIdMapping
- uniqueUserIdMapping
- userDisplayNameMapping
- userSecurityNameMapping
- supportedEntityType
  - defaultParent
  - name

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
maxSearchResults	int	4500	Maximum number of entries that can be returned in a search.
pageCacheSize	int	1000	Defines the number of pagination requests that can be stored in the cache. The paging cache size needs to be configured based on the number of pagination requests executed on the system and the hardware system resources available.
pageCacheTimeout	A period of time with millisecond precision	30000ms	Defines the maximum time that an entry, which added to the page cache, is available. When the specified time has elapsed, the entry from the page cache is cleared. This needs to be configured based on the interval between pagination search requests executed on the system and the hardware system resources available. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
searchTimeout	A period of time with millisecond precision	10m	Maximum amount of time, in milliseconds, to process a search. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

### extendedProperty

The extended properties for Person and Group.

false

Attribute name	Data type	Default value	Description
dataType	<ul style="list-style-type: none"> <li>• Double</li> <li>• Long</li> <li>• Date</li> <li>• String</li> <li>• BigDecimal</li> <li>• BigInteger</li> <li>• Boolean</li> <li>• Integer</li> </ul>		<p>Defines the data type of the property extended for Person and Group. The basic Java data types are supported.</p> <p><b>Double</b> Double</p> <p><b>Long</b> Long</p> <p><b>Date</b> Date</p> <p><b>String</b> String</p> <p><b>BigDecimal</b> BigDecimal</p> <p><b>BigInteger</b> BigInteger</p> <p><b>Boolean</b> Boolean</p> <p><b>Integer</b> Integer</p>
defaultValue	string		Defines the default value for the property during write operation, if no default value is set.
entityType	<ul style="list-style-type: none"> <li>• PersonAccount</li> <li>• Group</li> </ul>		<p>The name of the entity being mapped. The name of the entity can be PersonAccount or Group.</p> <p><b>PersonAccount</b> Person</p> <p><b>Group</b> Group</p>
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
multiValued	boolean	false	Defines if the property extended for Person and Group supports multiple values.
name	string		Defines the name of the property extended for Person and Group.

### **primaryRealm**

Primary realm configuration.

false

Attribute name	Data type	Default value	Description
allowOpIfRepoDown	boolean	false	Specifies whether operation is allowed if a repository is down. The default value is false.
delimiter	string	/	Delimiter used to qualify the realm under which the operation should be executed. For example, userid=test1/myrealm where / is the delimiter and myrealm is the realm name.
name	string		Name of the realm.

### **primaryRealm > defaultParents**

The default parent mapping for the realm.

false

Attribute name	Data type	Default value	Description
name	string		The name of the entity being mapped. The name of the entity can be PersonAccount or Group.
parentUniqueName	string		The distinguished name under Base distinguished name (DN) in the repository under which all entities of the configured type will be created.

### **primaryRealm > groupDisplayNameMapping**

The input and output property mappings for group display name in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	cn	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.
outputProperty	string	cn	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**primaryRealm > groupSecurityNameMapping**

The input and output property mappings for group security name in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	cn	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.
outputProperty	string	cn	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**primaryRealm > participatingBaseEntry**

The Base Entry that is part of this realm.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Name of the base entry.

**primaryRealm > uniqueGroupIdMapping**

The input and output property mappings for unique group id in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	cn	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.
outputProperty	string	uniqueName	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**primaryRealm > uniqueUserIdMapping**

The input and output property mappings for unique user id used in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	uniqueName	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.
outputProperty	string	uniqueName	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**primaryRealm > userDisplayNameMapping**

The input and output property mappings for user display name in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	principalName	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

Attribute name	Data type	Default value	Description
outputProperty	string	principalName	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**primaryRealm > userSecurityNameMapping**

The input and output property mappings for user security name in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	principalName	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.
outputProperty	string	uniqueName	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**realm**

Reference to the realm.

false

Attribute name	Data type	Default value	Description
allowOpIfRepoDown	boolean	false	Specifies whether operation is allowed if a repository is down. The default value is false.
delimiter	string	/	Delimiter used to qualify the realm under which the operation should be executed. For example, userid=test1/myrealm where / is the delimiter and myrealm is the realm name.
id	string		A unique configuration ID.
name	string		Name of the realm.

**realm > defaultParents**

The default parent mapping for the realm.

false

Attribute name	Data type	Default value	Description
name	string		The name of the entity being mapped. The name of the entity can be PersonAccount or Group.
parentUniqueName	string		The distinguished name under Base distinguished name (DN) in the repository under which all entities of the configured type will be created.

**realm > groupDisplayNameMapping**

The input and output property mappings for group display name in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	cn	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.
outputProperty	string	cn	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**realm > groupSecurityNameMapping**

The input and output property mappings for group security name in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	cn	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

Attribute name	Data type	Default value	Description
outputProperty	string	cn	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**realm > participatingBaseEntry**

The Base Entry that is part of this realm.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Name of the base entry.

**realm > uniqueGroupIdMapping**

The input and output property mappings for unique group id in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	cn	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.
outputProperty	string	uniqueName	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**realm > uniqueUserIdMapping**

The input and output property mappings for unique user id used in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	uniqueName	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

Attribute name	Data type	Default value	Description
outputProperty	string	uniqueName	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**realm > userDisplayNameMapping**

The input and output property mappings for user display name in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	principalName	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.
outputProperty	string	principalName	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**realm > userSecurityNameMapping**

The input and output property mappings for user security name in an user registry operation.

false

Attribute name	Data type	Default value	Description
inputProperty	string	principalName	The property that maps to the user registry attribute for input. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.
outputProperty	string	uniqueName	The property that maps to the user registry attribute for output. The valid values are: uniqueId, uniqueName, externalId, externalName and the attributes of PersonAccount and Group entity types.

**supportedEntityType**

The default parent for an entity type mapping.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

**supportedEntityType > defaultParent**

The distinguished name under Base distinguished name (DN) in the repository under which all entities of the configured type will be created.

false

string

**supportedEntityType > name**

The name of the entity being mapped. The name of the entity can be PersonAccount or Group.

false

string

## z/OS Connect File System Logger Interceptor (fileSystemLoggerInterceptor)

Defines a z/OS Connect File System logger interceptor.

Attribute name	Data type	Default value	Description
bufferSize	int	8192	Buffer size in bytes to be used when the bufferLogging attribute is set to true.
bufferedLogging	boolean	false	Indicates whether entries to the log is buffered before they are written to the log file.
encoding	string	UTF-8	Encoding used when writing to the log file.
id	string		A unique configuration ID.
logName	string		Log file name pattern used for payload logging.
logOption	<ul style="list-style-type: none"> <li>• RESPONSE</li> <li>• REQUEST</li> <li>• ALL</li> </ul>	ALL	<p>Log option that controls what is logged.</p> <p><b>RESPONSE</b> Indicates that only response data is logged.</p> <p><b>REQUEST</b> Indicates that only request data is logged.</p> <p><b>ALL</b> Indicates that both request and response data are logged.</p>

Attribute name	Data type	Default value	Description
logPath	string		File system location in which the file log is created. If the environment variable <code>\${server.output.dir}</code> is configured, its value is used by default.
maxPayloadSize	int	524288	Maximum payload size in characters allowed to be written to the log file.
rollOffLogPolicy	<ul style="list-style-type: none"> <li>• SIZE</li> <li>• DURATION</li> </ul>	SIZE	<p>Indicates that log file should be rolled off based on size or duration.</p> <p><b>SIZE</b> Indicates that the log file should be roll off based on the size of the log.</p> <p><b>DURATION</b> Indicates that the roll off log policy will be based on the elapsed time since the active log file was created.</p>
rollOffLogPolicyDuration	int	1440	Roll off policy duration in minutes.
rollOffLogPolicySize	int	52428800	Roll off policy size in bytes.
sequence	int Minimum: 0 Maximum: 2147483647	0	Sequence in which the interceptor is processed with respect to others.

## Fileset (fileset)

Specifies a set of files starting from a base directory and matching a set of patterns.

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	<code>\${server.config.dir}</code>	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

## Health Policy (healthPolicy)

Defines a condition for a server to be considered healthy and actions to take when the condition is not met.

- action
- cluster
- excessiveMemoryUsage
- excessiveRequestTimeout
- excessiveResponseTime
- host
- memoryLeak
- server

Attribute name	Data type	Default value	Description
enabled	boolean	true	Indicates whether the health policy is enabled.
id	string		A unique configuration ID.

### action

An action to take when the health condition breaches.

false

Attribute name	Data type	Default value	Description
action	<ul style="list-style-type: none"> <li>• generateThreadDump</li> <li>• restartServer</li> <li>• exitMaintenanceMode</li> <li>• enterMaintenanceMode</li> <li>• generateHeapDump</li> </ul>		<p>An action to take when the health condition breaches.</p> <p><b>generateThreadDump</b> Generate a thread dump of the server.</p> <p><b>restartServer</b> Restart the server.</p> <p><b>exitMaintenanceMode</b> Remove the server from maintenance mode</p> <p><b>enterMaintenanceMode</b> Put the server into maintenance mode</p> <p><b>generateHeapDump</b> Generate a heap dump of the server.</p>

#### cluster

Applies the health policy to servers that belong to a cluster.

false

Attribute name	Data type	Default value	Description
clusterName	string		The name of a cluster of servers to be monitored.

#### excessiveMemoryUsage

Detects if a JVM's heap size has grown over a configured percentage of the maximum heap size for a configured period of time.

false

Attribute name	Data type	Default value	Description
heapSizePercentage	int Minimum: 1 Maximum: 99	85	The threshold value for the percentage of the max heap size used by the server.

Attribute name	Data type	Default value	Description
timePeriod	A period of time with millisecond precision	5m	The time period over which the heap size must be over threshold before action is taken. The value can be from 1 millisecond to 1 day. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

#### **excessiveRequestTimeout**

Detects when the request timeout of a server, as measured by a web server that is enabled for Intelligent Management, exceeds the configured threshold value.

false

Attribute name	Data type	Default value	Description
timeoutPercentage	int Minimum: 1 Maximum: 99	85	The threshold value for the percentage of the request timeout by the server.

#### **excessiveResponseTime**

Detects when the average response time of requests to a server, as measured by a web server that is enabled for Intelligent Management, exceeds the configured threshold value.

false

Attribute name	Data type	Default value	Description
responseTime	A period of time with millisecond precision	10s	The average time that requests can take prior to corrective action. The value can be from 1 millisecond to 1 hour. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

#### **host**

Applies the health policy to servers that reside on a host.

false

Attribute name	Data type	Default value	Description
hostName	string		The name of a host whose servers are to be monitored.

**memoryLeak**

Detects if a JVMs heap size after the GC keeps growing.

false

**server**

Applies the health policy to a specific server.

false

Attribute name	Data type	Default value	Description
hostName	string		The host name of the server to be monitored.
serverName	string		The name of the server to be monitored.
wlpUsrDirectory	Path to a directory		The absolute WLP usr directory of the server to be monitored.

## Host Access (hostAccess)

Host Access configuration

Attribute name	Data type	Default value	Description
connTimeout	A period of time with second precision	180s	Amount of time to wait for obtaining a remote connection to remote targets. The default value is 180 seconds. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
enableCustomActions	boolean	false	Indicates whether custom actions are allowed to be executed on collective hosts. The default value is false.

Attribute name	Data type	Default value	Description
operationTimeout	A period of time with second precision	360s	Amount of time to wait for completing an operation on remote targets. The default value is 360 seconds. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
useSftp	boolean	false	Indicates whether to use sftp to transfer file. Te default value is false meaning to use scp to transfer file.

## Host Authentication Information (hostAuthInfo)

Connection details to allow for the collective controller to authenticate to the server's host.

Attribute name	Data type	Default value	Description
rpcHost	string	localhost	The fully qualified host name or IP address. A '*' wildcard will result in host name detection; this is not recommended for multi-homed systems and may result in unexpected behaviour. The host name must be unique within the network and must be the host name on which the remote connection protocol is listening (SSH, or OS specific RPC). This value will inherit from the defaultHostName variable if not set. The host name set here will directly control where the server's information is stored within the collective controller repository.
rpcPort	int	22	The port on which the remote connection protocol is listening (SSH, or OS specific RPC). See product documentation for supported RPC mechanisms.

Attribute name	Data type	Default value	Description
rpcUser	string		The operating system user ID to use to connect to the host.
rpcUserHome	string		The home directory of the user login ID. Only required to be set if sudo is to be used and SSH generation is to be done automatically.
rpcUserPassword	Reversably encoded password (string)		The password for the operating system user. If this property is not set, key-based authentication will be used. Use of key-based authentication is recommended for hosts which support SSH. If this property is set and sshPrivateKeyPath is also set, the key will take precedence.
sshPrivateKeyPassword	Reversably encoded password (string)		The password for the SSH private key.
sshPrivateKeyPath	string		The path to the SSH private key file. If the key pair does not exist, a key pair will be generated automatically. The private key is required for key-based authentication.
sshPublicKeyPath	string		The path to the SSH public key file. If the key pair does not exist, a key pair will be generated automatically. The public key will be placed into the configured userId's authorized_keys file if it is not present. Setting the path to the public key is not required.
sudoUser	string		The sudo user ID. This property should not be set when useSudo=false.
sudoUserPassword	Reversably encoded password (string)		The password for the sudo user. This property should not be set when useSudo=false.

Attribute name	Data type	Default value	Description
useHostCredentials	boolean		If this property is set to true, then the product uses the RPC credentials of the host to invoke commands and ignores other parameters in the 'Host Authentication Information' element.
useSudo	boolean		If this property is set to true, then sudo will be used to invoke commands. The user to sudo as can be controlled by setting sudoUser attribute. If sudoUser is not set, then the user to sudo as will be the configured default sudo user for the host. If this property is not set, and either sudoUser or sudoUserPassword are set, then useSudo is assumed to be true. If this property is set to false, and either sudoUser or sudoUserPassword are set, then a warning will be printed and the sudo options will be ignored.

## Host Singleton (hostSingleton)

Host singleton elector configuration

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string	*	The name of the singleton. A '*' wildcard is the default value and indicates this configuration applies to all singletons in this server.
port	int	0	The port to use for host singleton leader elections. A value of 0 is the default and means that no election will occur. In this case, the singleton in each member will be its own leader.

## HTTP Access Logging (httpAccessLogging)

HTTP access logs contain a record of all inbound HTTP client requests.

Attribute name	Data type	Default value	Description
enabled	boolean	true	Enable access logging.

Attribute name	Data type	Default value	Description
filePath	Path to a file	\${server.output.dir}/logs/http_access.log	Directory path and name of the access log file. Standard variable substitutions, such as \${server.output.dir}, can be used when specifying the directory path.
id	string		A unique configuration ID.
logFormat	string	%h %u %t]W "%r" %s %b	Specifies the log format that is used when logging client access information.
maxFileSize	int Minimum: 0	20	Maximum size of a log file, in megabytes, before being rolled over; a value of 0 means no limit.
maxFiles	int Minimum: 0	2	Maximum number of log files that will be kept, before the oldest file is removed; a value of 0 means no limit.

## HTTP Dispatcher (httpDispatcher)

HTTP Dispatcher configuration.

- trustedHeaderOrigin

Attribute name	Data type	Default value	Description
appOrContextRootMissingMessage	string		Message to return to the client when the application in the requested URI can not be found.
enableWelcomePage	boolean	true	Enables the default Liberty profile welcome page when no application is bound to a context root of "/". The default value is true.

### trustedHeaderOrigin

Private headers are used by the web server plug-in to provide information about the original request. These headers take precedence over the http Host header, and are used to select a virtual host to service a request. The default value is '\*', which will trust incoming private headers from any source. Specify 'none' to disable private headers and rely only on the http Host header, or specify a list of IP addresses to restrict private header processing to specific trusted sources.

false

string

## HTTP Transport Encoding (httpEncoding)

HTTP transport encoding settings

Attribute name	Data type	Default value	Description
converter.Big5	string	Cp950	Big5 Chinese converter

Attribute name	Data type	Default value	Description
converter.EUC-JP	string	Cp33722C	EUC Japanese converter (EUC-JP)
converter.EUC-KR	string	Cp970	EUC Korean converter (EUC-KR)
converter.EUC-TW	string	Cp964	EUC Chinese (Taiwan) converter (EUC-TW)
converter.EUC_KR	string	Cp970	EUC Korean converter (EUC_KR)
converter.GB2312	string	EUC_CN	GB2312 Chinese converter
converter.ISO-2022-KR	string	ISO2022KR	ISO-2022 Korean converter (ISO-2022-KR)
converter.Shift_JIS	string	Cp943C	Shift_JIS Japanese converter
encoding.ar	string	ISO-8859-6	Arabic language encoding (ar)
encoding.be	string	ISO-8859-5	Belarusian language encoding (be)
encoding.bg	string	ISO-8859-5	Bulgarian language encoding (bg)
encoding.bn	string	UTF-8	Bengali language encoding (bn)
encoding.ca	string	ISO-8859-1	Catalan language encoding (ca)
encoding.cs	string	ISO-8859-2	Czech language encoding (cs)
encoding.da	string	ISO-8859-1	Danish language encoding (da)
encoding.de	string	ISO-8859-1	German language encoding (de)
encoding.el	string	ISO-8859-7	Greek language encoding (el)
encoding.en	string	ISO-8859-1	English language encoding (en)
encoding.es	string	ISO-8859-1	Spanish language encoding (es)
encoding.et	string	ISO-8859-4	Estonian language encoding (et)
encoding.eu	string	ISO-8859-1	Basque language encoding (eu)
encoding.fa	string	ISO-8859-6	Persian language encoding (fa)
encoding.fi	string	ISO-8859-1	Finnish language encoding (fi)
encoding.fo	string	ISO-8859-2	Faroese language encoding (fo)
encoding.fr	string	ISO-8859-1	French language encoding (fr)
encoding.he	string	ISO-8859-8	Hebrew language encoding (he)

Attribute name	Data type	Default value	Description
encoding.hi	string	UTF-8	Hindi language encoding (hi)
encoding.hr	string	ISO-8859-2	Croatian language encoding (hr)
encoding.hu	string	ISO-8859-2	Hungarian language encoding (hu)
encoding.hy	string	UTF-8	Armenian language encoding (hy)
encoding.is	string	ISO-8859-1	Icelandic language encoding (is)
encoding.it	string	ISO-8859-1	Italian language encoding (it)
encoding.iw	string	ISO-8859-8	Hebrew language encoding (iw)
encoding.ja	string	Shift_JIS	Japanese language encoding (ja)
encoding.ji	string	ISO-8859-8	Yiddish language encoding (ji)
encoding.ka	string	UTF-8	Georgian language encoding (ka)
encoding.ko	string	EUC-KR	Korean language encoding (ko)
encoding.lt	string	ISO-8859-2	Lithuanian language encoding (lt)
encoding.lv	string	ISO-8859-4	Latvian language encoding (lv)
encoding.mk	string	ISO-8859-5	Macedonian language encoding (mk)
encoding.mr	string	UTF-8	Marathi language encoding (mr)
encoding.ms	string	ISO-8859-6	Malay language encoding (ms)
encoding.mt	string	ISO-8859-3	Maltese language encoding (mt)
encoding.nl	string	ISO-8859-1	Dutch language encoding (nl)
encoding.no	string	ISO-8859-1	Norwegian language encoding (no)
encoding.pl	string	ISO-8859-2	Polish language encoding (pl)
encoding.pt	string	ISO-8859-1	Portuguese language encoding (pt)
encoding.ro	string	ISO-8859-2	Romanian language encoding (ro)
encoding.ru	string	ISO-8859-5	Russian language encoding (ru)
encoding.sa	string	UTF-8	Sanskrit language encoding (sa)

Attribute name	Data type	Default value	Description
encoding.sh	string	ISO-8859-2	Serbo-Croatian language encoding (sh)
encoding.sk	string	ISO-8859-2	Slovak language encoding (sk)
encoding.sl	string	ISO-8859-2	Slovenian language encoding (sl)
encoding.sq	string	ISO-8859-2	Albanian language encoding (sq)
encoding.sr	string	ISO-8859-5	Serbian language encoding (sr)
encoding.sv	string	ISO-8859-1	Swedish language encoding (sv)
encoding.ta	string	UTF-8	Tamil language encoding (ta)
encoding.th	string	windows-874	Thai language encoding (th)
encoding.tr	string	ISO-8859-9	Turkish language encoding (tr)
encoding.uk	string	ISO-8859-5	Ukrainian language encoding (uk)
encoding.vi	string	windows-1258	Vietnamese language encoding (vi)
encoding.yi	string	ISO-8859-8	Yiddish language encoding (yi)
encoding.zh	string	GB2312	Chinese language encoding (zh)
encoding.zh_TW	string	Big5	Chinese language encoding (zh_TW)

## HTTP Endpoint (`httpEndpoint`)

Configuration properties for an HTTP endpoint.

- `accessLogging`
- `httpOptions`
- `sslOptions`
- `tcpOptions`

Attribute name	Data type	Default value	Description
<code>accessLoggingRef</code>	A reference to top level <code>httpAccessLogging</code> element (string).		HTTP access logging configuration for the endpoint.
<code>enabled</code>	boolean	<code>true</code>	Toggle the availability of an endpoint. When true, this endpoint will be activated by the dispatcher to handle HTTP requests.

Attribute name	Data type	Default value	Description
host	string	localhost	IP address, domain name server (DNS) host name with domain name suffix, or just the DNS host name, used by a client to request a resource. Use '*' for all available network interfaces.
httpOptionsRef	A reference to top level httpOptions element (string).	defaultHttpOptions	HTTP protocol options for the endpoint.
httpPort	int Minimum: -1 Maximum: 65535		The port used for client HTTP requests. Use -1 to disable this port.
httpsPort	int Minimum: -1 Maximum: 65535		The port used for client HTTP requests secured with SSL (https). Use -1 to disable this port.
id	string		A unique configuration ID.
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Action to take after a failure to start an endpoint.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>
sslOptionsRef	A reference to top level sslOptions element (string).		SSL protocol options for the endpoint.
tcpOptionsRef	A reference to top level tcpOptions element (string).	defaultTCPOptions	TCP protocol options for the endpoint.

### accessLogging

HTTP access logging configuration for the endpoint.

false

Attribute name	Data type	Default value	Description
enabled	boolean	true	Enable access logging.
filePath	Path to a file	\${server.output.dir}/logs/http_access.log	Directory path and name of the access log file. Standard variable substitutions, such as \${server.output.dir}, can be used when specifying the directory path.
logFormat	string	%h %u %{t}W "%r" %s %b	Specifies the log format that is used when logging client access information.
maxFileSize	int Minimum: 0	20	Maximum size of a log file, in megabytes, before being rolled over; a value of 0 means no limit.
maxFiles	int Minimum: 0	2	Maximum number of log files that will be kept, before the oldest file is removed; a value of 0 means no limit.

### httpOptions

HTTP protocol options for the endpoint.

false

Attribute name	Data type	Default value	Description
keepAliveEnabled	boolean	true	Enables persistent connections (HTTP keepalive). If true, connections are kept alive for reuse by multiple sequential requests and responses. If false, connections are closed after the response is sent.
maxKeepAliveRequests	int Minimum: -1	100	Maximum number of persistent requests that are allowed on a single HTTP connection if persistent connections are enabled. A value of -1 means unlimited.

Attribute name	Data type	Default value	Description
persistTimeout	A period of time with second precision	30s	Amount of time that a socket will be allowed to remain idle between requests. This setting only applies if persistent connections are enabled. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
readTimeout	A period of time with second precision	60s	Amount of time to wait for a read request to complete on a socket after the first read occurs. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
removeServerHeader	boolean	false	Removes server implementation information from HTTP headers and also disables the default Liberty profile welcome page.
writeTimeout	A period of time with second precision	60s	Amount of time to wait on a socket for each portion of the response data to be transmitted. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

### sslOptions

SSL protocol options for the endpoint.

false

Attribute name	Data type	Default value	Description
sessionTimeout	A period of time with second precision	1d	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
sslRef	A reference to top level ssl element (string).		The default SSL configuration repertoire. The default value is defaultSSLSettings.
suppressHandshakeErrors	boolean	false	Disable logging of SSL handshake errors. SSL handshake errors can occur during normal operation, however these messages can be useful when SSL is behaving unexpectedly.

### tcpOptions

TCP protocol options for the endpoint.

false

Attribute name	Data type	Default value	Description
inactivityTimeout	A period of time with millisecond precision	60s	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
soReuseAddr	boolean	true	Enables immediate rebind to a port with no active listener.

## HTTP Options (httpOptions)

HTTP protocol configuration.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
keepAliveEnabled	boolean	true	Enables persistent connections (HTTP keepalive). If true, connections are kept alive for reuse by multiple sequential requests and responses. If false, connections are closed after the response is sent.
maxKeepAliveRequests	int Minimum: -1	100	Maximum number of persistent requests that are allowed on a single HTTP connection if persistent connections are enabled. A value of -1 means unlimited.
persistTimeout	A period of time with second precision	30s	Amount of time that a socket will be allowed to remain idle between requests. This setting only applies if persistent connections are enabled. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
readTimeout	A period of time with second precision	60s	Amount of time to wait for a read request to complete on a socket after the first read occurs. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
removeServerHeader	boolean	false	Removes server implementation information from HTTP headers and also disables the default Liberty profile welcome page.

Attribute name	Data type	Default value	Description
writeTimeout	A period of time with second precision	60s	Amount of time to wait on a socket for each portion of the response data to be transmitted. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

## HTTP Proxy Redirect (httpProxyRedirect)

Configures port redirection. HTTP Proxy Redirect is used when redirecting HTTP requests from a non-secure port (for example, 80) to an SSL-enabled secured port (for example, 443).

Attribute name	Data type	Default value	Description
enabled	boolean	true	This attribute determines whether or not the server should redirect ports that are specified in this configuration element. The default is true.
host	string	*	The host name used for this proxy redirect. The server redirects HTTP requests only if the incoming request specifies a host name that matches this value. The default is * (all hosts).
httpPort	int Minimum: 1 Maximum: 65535		The (non-secure) port to redirect from. Incoming HTTP requests on this port are redirected to the specified HTTPS port.
httpsPort	int Minimum: 1 Maximum: 65535		The (secure) port to redirect to. Incoming HTTP requests that use the HTTP port are redirected to this port.
id	string		A unique configuration ID.

## HTTP Session (httpSession)

Configuration for HTTP session management.

Attribute name	Data type	Default value	Description
allowOverflow	boolean	true	Allows the number of sessions in memory to exceed the value of the Max in-memory session count property.
alwaysEncodeUrl	boolean	false	The Servlet 2.5 specification specifies to not encode the URL on a response.encodeURL call if it is not necessary. To support backward compatibility when URL encoding is enabled, set this property to true to call the encodeURL method. The URL is always encoded, even if the browser supports cookies.
cloneId	string		The clone identifier of the cluster member. Within a cluster, this identifier must be unique to maintain session affinity. When set, this name overwrites the default name generated by the server.

Attribute name	Data type	Default value	Description
cloneSeparator	string	:	The single character used to separate the session identifier from the clone identifier in session cookies. The default value should usually be used. On some Wireless Application Protocol (WAP) devices, a colon (:) is not allowed, so a plus sign (+) should be used instead. Different values should rarely be used. You should understand the clone character requirements of other products running on your system before using this property to change the clone separator character. The fact that any character can be specified as the value for this property does not imply that the character you specify will function correctly. This fact also does not imply that IBM is responsible for fixing any problem that might arise from using an alternative character.
cookieDomain	string		Domain field of a session tracking cookie.
cookieHttpOnly	boolean	true	Specifies that session cookies include the HttpOnly field. Browsers that support the HttpOnly field do not enable cookies to be accessed by client-side scripts. Using the HttpOnly field will help prevent cross-site scripting attacks.
cookieMaxAge	A period of time with second precision	-1	Maximum amount of time that a cookie can reside on the client browser. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
cookieName	string	JSESSIONID	A unique name for a session management cookie.

Attribute name	Data type	Default value	Description
cookiePath	string	/	A cookie is sent to the URL designated in the path.
cookieSecure	boolean	false	Specifies that the session cookies include the secure field.
cookiesEnabled	boolean	true	Specifies that session tracking uses cookies to carry session identifiers.
debugCrossover	boolean	false	Enable this option to perform additional checks to verify that only the session associated with the request is accessed or referenced, and log messages if any discrepancies are detected. Disable this option to skip the additional checks.
forceInvalidationMultiple	int	3	If your requests normally are not bound by a response time limit, specify 0 to indicate that the session manager should wait indefinitely until a request is complete before attempting to invalidate the session. Otherwise, set this property to a positive integer to delay the invalidation of active sessions. Active timed out sessions will not be invalidated by the first invalidation interval pass, but will be invalidated by the interval pass based on this value. For example, a value of 2 would invalidate an active session on the second invalidation interval pass after the session timeout has expired.
idLength	int	23	Length of the session identifier.

Attribute name	Data type	Default value	Description
idReuse	boolean	false	In a multi-JVM environment that is not configured for session persistence, setting this property to "true" enables the session manager to use the same session information for all of a user's requests even if the web applications that are handling these requests are governed by different JVMs. The default value for this property is false. Set this property to true if you want to enable the session manager to use the session identifier sent from a browser to preserve session data across web applications that are running in an environment that is not configured for session persistence.
invalidateOnUnauthorizedSessionRequestException	boolean	false	Set this property to true if, in response to an unauthorized request, you want the session manager to invalidate a session instead of issuing an UnauthorizedSessionRequestException. When a session is invalidated, the requester can create a new session, but does not have access to any of the previously saved session data. This allows a single user to continue processing requests to other applications after a logout while still protecting session data.
invalidationTimeout	A period of time with second precision	30m	Amount of time a session can go unused before it is no longer valid. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
maxInMemorySessionCount	int	1000	Maximum number of sessions to maintain in memory for each web module.
noAdditionalInfo	boolean	false	Forces removal of information that is not needed in session identifiers.
protocolSwitchRewritingEnabled	boolean	false	Adds the session identifier to a URL when the URL requires a switch from HTTP to HTTPS or from HTTPS to HTTP.
reaperPollInterval	A period of time with second precision	-1	The wake-up interval, in seconds, for the process that removes invalid sessions. The minimum value is 30 seconds. If a value less than the minimum is entered, an appropriate value is automatically determined and used. This value overrides the default installation value, which is between 30 and 360 seconds, based off the session timeout value. Because the default session timeout is 30 minutes, the reaper interval is usually between 2 and 3 minutes. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
rewriteId	string	jsessionId	Use this property to change the key used with URL rewriting.
securityIntegrationEnabled	boolean	true	Enables security integration, which causes the session management facility to associate the identity of users with their HTTP sessions.

Attribute name	Data type	Default value	Description
securityUserIgnoreCase	boolean	false	Indicates that the session security identity and the client security identity should be considered a match even if their cases are different. For example, when this property is set to true, the session security identity USER1 matches the client security identities User1 and user1.
sslTrackingEnabled	boolean	false	Specifies that session tracking uses Secure Sockets Layer (SSL) information as a session identifier.
urlRewritingEnabled	boolean	false	Specifies that the session management facility uses rewritten URLs to carry the session identifiers.
useContextRootAsCookiePath	boolean	false	Specifies that the cookie path equals the context root of the web module instead of /

## HTTP Session Database (httpSessionDatabase)

Controls how HTTP sessions are persisted to a database.

Attribute name	Data type	Default value	Description
dataSourceRef	string		The identifier of the data source the session manager should use to persist HTTP session data.

Attribute name	Data type	Default value	Description
db2RowSize	<ul style="list-style-type: none"> <li>• 32KB</li> <li>• 4KB</li> <li>• 8KB</li> <li>• 16KB</li> </ul>	4KB	<p>Table space page size configured for the sessions table, if using a DB2 database. Increasing this value can improve database performance in some environments.</p> <p><b>32KB</b> Use a table space page size of 32 KB. You must additionally create a DB2 buffer pool and table space, and specify 32KB as the page size for both. You must also specify the name of the table space you created.</p> <p><b>4KB</b> Use the default table space page size of 4 KB. You do not need to create a DB2 buffer pool or table space, and you do not need to specify a table space name.</p> <p><b>8KB</b> Use a table space page size of 8 KB. You must additionally create a DB2 buffer pool and table space, and specify 8KB as the page size for both. You must also specify the name of the table space you created.</p> <p><b>16KB</b> Use a table space page size of 16 KB. You must additionally create a DB2 buffer pool and table space, and specify 16KB as the page size for both. You must also specify the name of the table space you created.</p>

Attribute name	Data type	Default value	Description
noAffinitySwitchBack	boolean	false	Set this property to "true" to maintain affinity to the new member even after original one comes back up. When a cluster member fails, its requests routed to a different cluster member, and sessions are activated in that other member. Thus, session affinity is maintained to the new member, and when failed cluster member comes back up, the requests for sessions that were created in the original cluster member are routed back to it. Allowed values are true or false, with the default being false. Set this property to true when you have distributed sessions configured with time-based write. Note that this property has no affect on the behavior when distributed sessions are not enabled.
onlyCheckInCacheDuringPrehook	boolean	false	A value of true indicates that the last access time of a session should only be updated if a request gets the session. A value of false indicates that the last access time of a session should be updated upon every request. Changing this value can improve performance in some environments.

Attribute name	Data type	Default value	Description
optimizeCacheIdIncrements	boolean	true	If the user's browser session is moving back and forth across multiple web applications, you might see extra persistent store activity as the in-memory sessions for a web module are refreshed from the persistent store. As a result, the cache identifiers are continually increasing and the in-memory session attributes are overwritten by those of the persistent copy. Set this property to true if you want to prevent the cache identifiers from continually increasing. A value of true indicates that the session manager should assess whether the in-memory session for a web module is older than the copy in persistent store. If the configuration is a cluster, ensure that the system times of each cluster member are as identical as possible.
scheduleInvalidation	boolean	false	Enable this option to reduce the number of database updates required to keep the HTTP sessions alive. Specify the two hours of a day when there is the least activity in the application server. When this option is disabled, the invalidator process runs every few minutes to remove invalidated HTTP sessions.
scheduleInvalidationFirstHour	int	0	Indicates the first hour during which the invalidated sessions are cleared from the persistent store. Specify this value as an integer between 0 and 23. This value is valid only when schedule invalidation is enabled.

Attribute name	Data type	Default value	Description
scheduleInvalidationSecondHour	int	0	Indicates the second hour during which the invalidated sessions are cleared from the persistent store. Specify this value as an integer between 0 and 23. This value is valid only when schedule invalidation is enabled.
skipIndexCreation	boolean	false	Set this property to "true" to disable index creation on server startup. This custom property should only be used if you want to manually create your own database indices for session persistence. However, it is recommended that you let session manager create database indices. Before enabling this property, make sure that the correct index does exist on your session database.
tableName	string	sessions	The database table name.
tableSpaceName	string		Table space to be used for the sessions table. This value is only required when the DB2 Row Size is greater than 4KB.
useInvalidatedId	boolean	true	Set this property to "true" to reuse the incoming identifier if the session with that identifier was recently invalidated. This is a performance optimization because it prevents checking the persistent store.
useMultiRowSchema	boolean	false	When enabled, each session data attribute is placed in a separate row in the database, allowing larger amounts of data to be stored for each session. This configuration can yield better performance when session attributes are very large and few changes are required to the session attributes. When disabled, all session data attributes are placed in the same row for each session.

Attribute name	Data type	Default value	Description
useOracleBlob	boolean	false	Set this property to "true" to create the database table using the Binary Large Object (BLOB) data type for the medium column. This value increases performance of persistent sessions when Oracle databases are used. Due to an Oracle restriction, BLOB support requires use of the Oracle Call Interface (OCI) database driver for more than 4000 bytes of data. You must also ensure that a new sessions table is created before the server is restarted by dropping your old sessions table or by changing the datasource definition to reference a database that does not contain a sessions table.
usingCustomSchemaName	boolean	false	Set this property to "true" if you are using DB2 for session persistence and the currentSchema property is set in the data source.
writeContents	<ul style="list-style-type: none"> <li>• ALL_SESSION_ATTRIBUTES</li> <li>• ONLY_UPDATED_ATTRIBUTES</li> </ul>	ONLY_UPDATED_ATTRIBUTES	<p>Specifies how much session data should be written to the persistent store. By default, only updated attributes are written, but all attributes can be written instead (regardless of whether or not they changed).</p> <p><b>ALL_SESSION_ATTRIBUTES</b> All attributes are written to the persistent store.</p> <p><b>ONLY_UPDATED_ATTRIBUTES</b> Only updated attributes are written to the persistent store.</p>

Attribute name	Data type	Default value	Description
writeFrequency	<ul style="list-style-type: none"> <li>• TIME_BASED_WRITE</li> <li>•</li> <li>END_OF_SERVLET_SERVICE</li> <li>• MANUAL_UPDATE</li> </ul>	END_OF_SERVLET_SERVICE	<p>Specifies when session data is written to the persistent store. By default, session data is written to the persistent store after the servlet completes execution. Changing this value can improve performance in some environments.</p> <p><b>TIME_BASED_WRITE</b> Session data is written to the persistent store based on the specified write interval value.</p> <p><b>END_OF_SERVLET_SERVICE</b> Session data is written to the persistent store after the servlet completes execution.</p> <p><b>MANUAL_UPDATE</b> A programmatic sync on the IBMSession object is required to write the session data to the persistent store.</p>
writeInterval	A period of time with second precision	2m	Number of seconds that should pass before writing session data to the persistent store. The default is 120 seconds. This value is only used when a time based write frequency is enabled. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

## HTTP Whiteboard (httpWhiteboard)

The HTTP Whiteboard provides a runtime environment for hosting servlets and resources provided by OSGi services.

Attribute name	Data type	Default value	Description
contextPath	string	/osgi/http	The context path to use for the HTTP Whiteboard runtime environment.

## IBM Tivoli Directory Server LDAP Filters (idsLdapFilterProperties)

Specifies the list of default IBM Tivoli Directory Server LDAP filters.

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)( (objectclass=groupOfNames)(objectclass=groupOfUniqueNames)(objectclass=groupOfNames))	An LDAP filter clause for searching the user registry for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	ibm-allGroups:member;ibm-allGroups:uniqueMember;groupOfNames:cn;groupOfUniqueNames:uniqueMember	An LDAP filter that maps group memberships to LDAP entries.
id	string		A unique configuration ID.
userFilter	string	(&(uid=%v)(objectclass=ePerson))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	*:uid	An LDAP filter that maps the name of a user to an LDAP entry.

## IIOE Endpoint (iiopEndpoint)

IIOE Endpoint configuration

- iiopOptions
- tcpOptions

Attribute name	Data type	Default value	Description
host	string	localhost	IP address, domain name server (DNS) host name with domain name suffix, or just the DNS host name
id	string		A unique configuration ID.
iiopPort	int		Port for the unsecured server socket opened by this IIOE endpoint
tcpOptionsRef	A reference to top level tcpOptions element (string).	defaultTCPOptions	TCP protocol options for the IIOE endpoint

### iiopOptions

Specification of a secured server socket opened by this IIOE endpoint

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
iiopsPort	int		Specify the port to be configured with the SSL options.
sessionTimeout	A period of time with second precision	1d	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
sslRef	A reference to top level ssl element (string).		The default SSL configuration repertoire. The default value is defaultSSLSettings.
suppressHandshakeErrors	boolean	false	Disable logging of SSL handshake errors. SSL handshake errors can occur during normal operation, however these messages can be useful when SSL is behaving unexpectedly.

### tcpOptions

TCP protocol options for the IIOP endpoint

false

Attribute name	Data type	Default value	Description
inactivityTimeout	A period of time with millisecond precision	60s	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
soReuseAddr	boolean	true	Enables immediate rebind to a port with no active listener.

## IIOp Server Policies (iiopServerPolicies)

Configuration for IIOp server policies

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

### Include (include)

Specify a configuration resource to include in the server's configuration.

Attribute name	Data type	Default value	Description
location	A file, directory or url.		Specifies the resource location. This can be a file path or a URI for a remote resource.
onConflict	<ul style="list-style-type: none"><li>• IGNORE</li><li>• REPLACE</li><li>• MERGE</li></ul>	MERGE	<p>Specifies the behavior that is used to merge elements when conflicts are found.</p> <p><b>IGNORE</b> Conflicting elements in the included file will be ignored.</p> <p><b>REPLACE</b> When elements conflict, the element from the included file will replace the conflicting element.</p> <p><b>MERGE</b> Conflicting elements will be merged together.</p>
optional	boolean	false	Allow the included resource to be skipped if it cannot be found.

## Installable (installable)

The installable configuration element

Attribute name	Data type	Default value	Description
expand	string		Specifies whether to expand the installable during deployment. Valid values are yes, no, or auto. Overrides the default behavior determined by the installable file type. A no value disables unzip for installable zip files. The default value is auto, which determines whether to expand or not expand based on the installable file type. For example, auto selects to expand the zip file type.
id	string		A unique configuration ID.
installDir	string		Absolute path to the installable target directory.
name	string	default	The name of the installable archive file, for example, wlp.8555.zip.
sourceDir	string		Absolute path to the installable archive file. The default value is the path: <code>\${WLP_STACK_GROUPS_DIR}/stack_name/installables</code>
type	string		The installable type. Valid values are wlp, jre, or other. This attribute overrides the type prefix of the installable name.

## Sun Java System Directory Server LDAP Filters (iplanetLdapFilterProperties)

Specifies the list of default Sun Java System Directory Server LDAP filters.

Attribute name	Data type	Default value	Description
groupFilter	string	<code>(&amp;(cn=%v)(objectclass=ldapsubentry))</code>	An LDAP filter clause for searching the user registry for groups.
groupIdMap	string	<code>*:cn</code>	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	<code>nsRole:nsRole</code>	An LDAP filter that identifies user to group memberships.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
userFilter	string	(&(uid=%v)(objectclass=inetOrgPerson))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	inetOrgPerson:uid	An LDAP filter that maps the name of a user to an LDAP entry.

## JAAS Login Context Entry (jaasLoginContextEntry)

The JAAS login context entry configuration.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
loginModuleRef	List of references to top level jaasLoginModule elements (comma-separated string).	hashtable,userNameAndPassword,certificate,lockID	A reference to the ID of a JAAS login module.
name	string		Name of a JAAS configuration entry.

## JAAS Login Module (jaasLoginModule)

A login module in the JAAS configuration.

- library
  - file
  - fileset
  - folder
- options

Attribute name	Data type	Default value	Description
className	string		Fully-qualified package name of the JAAS login module class.

Attribute name	Data type	Default value	Description
controlFlag	<ul style="list-style-type: none"> <li>• SUFFICIENT</li> <li>• REQUISITE</li> <li>• REQUIRED</li> <li>• OPTIONAL</li> </ul>	REQUIRED	<p>The login module's control flag. Valid values are REQUIRED, REQUISITE, SUFFICIENT, and OPTIONAL.</p> <p><b>SUFFICIENT</b> This LoginModule is SUFFICIENT as per the JAAS specification. The LoginModule is not required to succeed. If authentication is successful, no other LoginModules will be called and control is returned to the caller.</p> <p><b>REQUISITE</b> This LoginModule is REQUISITE as per the JAAS specification. The LoginModule is required to succeed. If authentication fails, no other LoginModules will be called and control is returned to the caller.</p> <p><b>REQUIRED</b> This LoginModule is REQUIRED as per the JAAS specification. The LoginModule is required to succeed.</p> <p><b>OPTIONAL</b> This LoginModule is OPTIONAL as per the JAAS specification. The LoginModule is not required to succeed.</p>
id	string		A unique configuration ID.
libraryRef	A reference to top level library element (string).		A reference to the ID of the shared library configuration.

## library

A reference to the ID of the shared library configuration.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

### library > file

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

### library > fileset

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

### library > folder

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

### options

A collection of JAAS Login module options

false

## Java 2 Security (javaPermission)

Configuration of permissions for Java 2 Security.

Attribute name	Data type	Default value	Description
actions	string		The actions that the permission grant allows on the target name. For example, read in the case of a java.io.FilePermission.
className	string		The name of the class implementing the permission being granted. For example, java.io.FilePermission.
codebase	string		The codebase that is being granted the permission.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
name	string		The target for which the permission applies to. For example, ALL FILES in the case of a java.io.FilePermission.
principalName	string		The principal to whom the permission is being granted.
principalType	string		The class name that would be matched for the given Principal Name.
restriction	boolean	false	Declares whether the permission is being restricted versus granted. If restriction is set to "true" then this permission is denied as opposed to being granted.

## JDBC Driver (jdbcDriver)

Identifies a JDBC driver.

- library
  - file
  - fileset
  - folder

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
javax.sql.ConnectionPoolDataSource	string		JDBC driver implementation of javax.sql.ConnectionPoolDataSource.
javax.sql.DataSource	string		JDBC driver implementation of javax.sql.DataSource.
javax.sql.XADataSource	string		JDBC driver implementation of javax.sql.XADataSource.
libraryRef	A reference to top level library element (string).		Identifies JDBC driver JARs and native files.

### library

Identifies JDBC driver JARs and native files.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

### library > file

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

### library > fileset

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

## JMS Activation Specification (jmsActivationSpec)

Defines a JMS activation specification configuration.

- authData
- properties.wasJms
- properties.wmqJms

Attribute name	Data type	Default value	Description
authDataRef	A reference to top level authData element (string).		Default authentication data for an activation specification.
id	string		A unique configuration ID.
maxEndpoints	int Minimum: 0	500	The maximum number of endpoints to dispatch to.

**authData**

Default authentication data for an activation specification.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

### properties.wasJms

A JMS activation specification is associated with one or more message-driven beans and provides the configuration necessary for them to receive messages.

false

Attribute name	Data type	Default value	Description
acknowledgeMode	<ul style="list-style-type: none"> <li>• Dups-ok-acknowledge</li> <li>• Auto-acknowledge</li> </ul>	Auto-acknowledge	<p>The acknowledge mode indicates how a message received by a message-driven bean should be acknowledged.</p> <p><b>Dups-ok-acknowledge</b> Dups-ok-acknowledge</p> <p><b>Auto-acknowledge</b> Auto-acknowledge</p>
busName	string	defaultBus	The name of a bus when connecting to the service integration bus in a full profile server.
clientId	string		The JMS client identifier needed for durable(and for shared non-durable) topic subscriptions on all connections. This identifier is required if the application is doing durable(and for shared non-durable) publish/subscribe messaging.

Attribute name	Data type	Default value	Description
connectionFactoryLookup	string		This property can be used to specify the lookup name of an administratively-defined <code>javax.jms.ConnectionFactory</code> , <code>javax.jms.QueueConnectionFactory</code> or <code>javax.jms.TopicConnectionFactory</code> object that is used to connect to the JMS provider from which the endpoint (message-driven bean) can receive messages.
destination	string		Reference to a JMS destination
destinationLookup	string		This property can be used to specify the lookup name of the administratively-defined <code>javax.jms.Queue</code> or <code>javax.jms.Topic</code> objects that define the JMS queue or topic from which the endpoint (message-driven bean) can receive messages.
destinationRef	A reference to top level <code>adminObject</code> element (string).		Reference to a JMS destination
destinationType	<ul style="list-style-type: none"> <li><code>javax.jms.Topic</code></li> <li><code>javax.jms.Queue</code></li> </ul>	<code>javax.jms.Queue</code>	The type of the destination, which is <code>javax.jms.Queue</code> or <code>javax.jms.Topic</code> .  <b>javax.jms.Topic</b> <code>javax.jms.Topic</code>  <b>javax.jms.Queue</b> <code>javax.jms.Queue</code>
maxBatchSize	int Minimum: 1 Maximum: 2147483647		The maximum number of messages received from the messaging engine in a single batch.
maxConcurrency	int Minimum: 1 Maximum: 2147483647	5	The maximum number of endpoints to which the messages are delivered concurrently. The increase in the number can improve the performance, but it also increases the number of threads that are in use at the specified time. If the message order must be retained for all the failed deliveries, set the maximum concurrent endpoints value to 1.

Attribute name	Data type	Default value	Description
messageSelector	string		The JMS message selector used to determine which messages the message-driven bean receives. The value is a string that is used to select a subset of the available messages.
readAhead	<ul style="list-style-type: none"> <li>• AlwaysOff</li> <li>• Default</li> <li>• AlwaysOn</li> </ul>	Default	<p>Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.</p> <p><b>AlwaysOff</b> AlwaysOff</p> <p><b>Default</b> Default</p> <p><b>AlwaysOn</b> AlwaysOn</p>
remoteServerAddress	string		<p>The remote server address that has triplets separated by a comma, with the syntax hostName:portNumber:chainName, used to connect to a bootstrap server. For example, Merlin:7276:BootstrapBasicMessaging. If hostName is not specified, the default is localhost. If portNumber is not specified, the default is 7276. If chainName is not specified, the default is BootstrapBasicMessaging. Refer to the information center for more information.</p>
retryInterval	A period of time with second precision	30s	The delay (in seconds) between attempts to connect to a messaging engine, both for the initial connection, and any subsequent attempts to establish a better connection. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
shareDurableSubscription	string		Controls whether or not durable subscription can be shared across connections.
subscriptionDurability	<ul style="list-style-type: none"> <li>DurableShared</li> <li>Durable</li> <li>NonDurable</li> <li>NonDurableShared</li> </ul>	NonDurable	<p>Type of MS topic subscription. The value can be any of following values: Durable DurableShared NonDurable NonDurableShared</p> <p><b>DurableShared</b> DurableShared</p> <p><b>Durable</b> Durable</p> <p><b>NonDurable</b> NonDurable</p> <p><b>NonDurableShared</b> NonDurableShared</p>
subscriptionName	string		The subscription name needed for durable(and for shared non-durable). Required field when using a durable(and for shared non-durable) topic subscription.This subscription name must be unique within a given client identifier.
targetTransportChain	<ul style="list-style-type: none"> <li>InboundSecureMessaging</li> <li>InboundBasicMessaging</li> </ul>	InboundBasicMessaging	<p>Transport chains specify the communication protocols that can be used to communicate with the service integration bus in a full profiles server.</p> <p><b>InboundSecureMessaging</b> InboundSecureMessaging</p> <p><b>InboundBasicMessaging</b> InboundBasicMessaging</p>

#### properties.wmqJms

WebSphere MQ JMS activation specification

false

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	819	The coded character set identifier for a connection.
applicationName	string		The name by which an application is registered with the queue manager.

Attribute name	Data type	Default value	Description
brokerCCDurSubQueue	string		The name of the queue from which non-durable subscription messages are retrieved for a ConnectionConsumer
brokerCCSubQueue	string		The name of the queue from which a connection consumer receives nondurable subscription messages
brokerControlQueue	string		The name of the broker control queue
brokerPubQueue	string		The name of the queue where published messages are sent (the stream queue)
brokerQueueManager	string		The name of the queue manager on which the broker is running
brokerSubQueue	string		The name of the queue from which a nondurable message consumer receives messages
brokerVersion	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>The version of the broker being used</p> <p>2      2</p> <p>1      1</p>
ccdtURL	string		A URL that identifies the name and location of the file containing the client channel definition table (CCDT) and specifies how the file can be accessed.
channel	string	SYSTEM.DEF.SVRCONN	The name of the MQI channel to use.
cleanupInterval	A period of time with millisecond precision		The interval, in milliseconds, between background runs of the publish/subscribe cleanup utility. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
cleanupLevel	<ul style="list-style-type: none"> <li>• SAFE</li> <li>• FORCE</li> <li>• NONDUR</li> <li>• NONE</li> <li>• STRONG</li> </ul>	SAFE	<p>The cleanup level for a broker-based subscription store.</p> <p><b>SAFE</b> SAFE</p> <p><b>FORCE</b> FORCE</p> <p><b>NONDUR</b> NONDUR</p> <p><b>NONE</b> NONE</p> <p><b>STRONG</b> STRONG</p>
clientId	string		The client identifier for a connection
cloneSupport	<ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	DISABLED	<p>Whether two or more instances of the same durable topic subscriber can run simultaneously</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DISABLED</b> DISABLED</p>
connectionNameList	string		<p>A list of TCP/IP connection names (hostname(port))used for communications. ConnectionNameList supersedes the hostname and port properties.</p>
destinationRef	A reference to top level adminObject element (string).		Destination
destinationType	<ul style="list-style-type: none"> <li>• javax.jms.Topic</li> <li>• javax.jms.Queue</li> </ul>	javax.jms.Queue	<p>The type of destination - javax.jms.Queue or javax.jms.Topic</p> <p><b>javax.jms.Topic</b> javax.jms.Topic</p> <p><b>javax.jms.Queue</b> javax.jms.Queue</p>
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state.
headerCompression	<ul style="list-style-type: none"> <li>• SYSTEM</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing header data on a connection</p> <p><b>SYSTEM</b> SYSTEM</p> <p><b>NONE</b> NONE</p>

Attribute name	Data type	Default value	Description
hostName	string	localhost	The host name or IP address of the system on which the queue manager resides. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.
localAddress	string		For a connection to a queue manager, this property specifies either or both of the following, (1) The local network interface to be used, (2) The local port, or range of local ports, to be used
maxMessages	int Minimum: 0	1	The maximum number of messages that can be assigned to a server session at one time. If the activation spec is delivering messages to an MDB in an XA transaction, a value of 1 is used regardless of the setting of this property.
maxPoolDepth	int Minimum: 0	10	The maxPoolDepth property on the activation specification defines the number of available MDB (Message Driven Bean) instances. Decreasing the value of this property decreases the number of messages that can be delivered concurrently.
messageBatchSize	int Minimum: 0		Maximum number of messages to process in one batch.
messageCompression	<ul style="list-style-type: none"> <li>• RLE</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing message data on a connection</p> <p><b>RLE</b> RLE</p> <p><b>NONE</b> NONE</p>
messageRetention	boolean		Whether the connection consumer keeps unwanted messages on the input queue

Attribute name	Data type	Default value	Description
messageSelection	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BROKER</li> </ul>	CLIENT	<p>Determines whether message selection is done by WebSphere MQ classes for JMS or by the broker.</p> <p><b>CLIENT</b> CLIENT</p> <p><b>BROKER</b> BROKER</p>
messageSelector	string		<p>Determines whether message selection is done by WebSphere MQ classes for JMS or by the broker. Message selection by the broker is not supported when brokerVersion has the value 1</p>
pollingInterval	A period of time with millisecond precision	5s	<p>If each message listener within a session has no suitable message on its queue, this value is the maximum interval, in milliseconds, that elapses before each message listener tries again to get a message from its queue. If it frequently happens that no suitable message is available for any of the message listeners in a session, consider increasing the value of this property. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.</p>

Attribute name	Data type	Default value	Description						
poolTimeout	A period of time with millisecond precision	5m	The time, in milliseconds, that an unused server session is held open in the server session pool before being closed due to inactivity. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.						
port	int Minimum: 1	1414	The port on which the queue manager listens. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.						
providerVersion	<ul style="list-style-type: none"> <li>• 7</li> <li>• 6</li> <li>• unspecified</li> </ul>	unspecified	<p>The version, release, modification level and fix pack of the queue manager to which the application intends to connect.</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50px;"><b>7</b></td> <td style="width: 50px;"><b>7</b></td> </tr> <tr> <td><b>6</b></td> <td><b>6</b></td> </tr> <tr> <td><b>unspecified</b></td> <td><b>unspecified</b></td> </tr> </table>	<b>7</b>	<b>7</b>	<b>6</b>	<b>6</b>	<b>unspecified</b>	<b>unspecified</b>
<b>7</b>	<b>7</b>								
<b>6</b>	<b>6</b>								
<b>unspecified</b>	<b>unspecified</b>								
queueManager	string		The name of the queue manager to connect to						
receiveCCSID	int Minimum: 0	0	Destination property that sets the target Coded character set identifier for queue manager message conversion. The value is ignored unless receive conversion is set to WMQ_RECEIVE_CONVERSION_QMG						
receiveConversion	<ul style="list-style-type: none"> <li>• QMGR</li> <li>• CLIENT_MSG</li> </ul>	CLIENT_MSG	<p>Destination property that determines if data conversion is going to be performed by the queue manager.</p> <p><b>QMGR</b> QMGR</p> <p><b>CLIENT_MSG</b> CLIENT_MSG</p>						

Attribute name	Data type	Default value	Description
receiveExit	string		Identifies a channel receive exit program, or a sequence of receive exit programs to be run in succession
receiveExitInit	string		The user data that is passed to channel receive exit programs when they are called
rescanInterval	A period of time with millisecond precision	5s	When a message consumer in the point-to-point domain uses a message selector to select which messages it wants to receive, WebSphere MQ classes for JMS searches the WebSphere MQ queue for suitable messages in the sequence determined by the <code>MsgDeliverySequence</code> attribute of the queue. When WebSphere MQ classes for JMS finds a suitable message and delivers it to the consumer, WebSphere MQ classes for JMS resumes the search for the next suitable message from its current position in the queue. WebSphere MQ classes for JMS continues to search the queue in this way until it reaches the end of the queue, or until the interval of time in milliseconds, as determined by the value of this property, has expired. In each case, WebSphere MQ classes for JMS returns to the beginning of the queue to continue its search, and a new time interval commences. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
securityExit	string		Identifies a channel security exit program

Attribute name	Data type	Default value	Description
securityExitInit	string		The user data that is passed to a channel security exit program when it is called
sendExit	string		Identifies a channel send exit program, or a sequence of send exit programs to be run in succession
sendExitInit	string		The user data that is passed to channel send exit programs when they are called
shareConvAllowed	boolean	true	Whether a client connection can share its socket with other top-level JMS connections from the same process to the same queue manager, if the channel definitions match
sparseSubscriptions	boolean	false	Controls the message retrieval policy of a TopicSubscriber object
sslCertStores	string		The Lightweight Directory Access Protocol (LDAP) servers that hold certificate revocation lists (CRLs) for use on an SSL connection
sslCipherSuite	string		The CipherSuite to use for an SSL connection
sslFipsRequired	boolean		Whether an SSL connection must use a CipherSuite that is supported by the IBM Java JSSE FIPS provider (IBMJSSEFIPS).
sslPeerName	string		For an SSL connection, a template that is used to check the distinguished name in the digital certificate provided by the queue manager
sslResetCount	int Minimum: 0 Maximum: 999999999	0	The total number of bytes sent and received by an SSL connection before the secret keys used by SSL are renegotiated

Attribute name	Data type	Default value	Description
startTimeout	A period of time with millisecond precision	10s	Configures the time duration (in milliseconds) within which the execution must start. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
statusRefreshInterval	A period of time with millisecond precision	1m	The interval, in milliseconds, between refreshes of the long running transaction that detects when a subscriber loses its connection to the queue manager. This property is relevant only if subscription store has the value QUEUE. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
subscriptionDurability	<ul style="list-style-type: none"> <li>• Durable</li> <li>• NonDurable</li> </ul>		<p>Whether a durable or nondurable subscription is used to deliver messages to an MDB subscribing to the topic</p> <p><b>Durable</b> Durable</p> <p><b>NonDurable</b> NonDurable</p>
subscriptionName	string		The name of the durable subscription

Attribute name	Data type	Default value	Description
subscriptionStore	<ul style="list-style-type: none"> <li>• MIGRATE</li> <li>• BROKER</li> <li>• QUEUE</li> </ul>	BROKER	Determines where WebSphere MQ classes for JMS stores persistent data about active subscriptions  <b>MIGRATE</b> MIGRATE  <b>BROKER</b> BROKER  <b>QUEUE</b> QUEUE
transportType	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BINDINGS</li> </ul>	CLIENT	Whether a connection to a queue manager uses client mode or bindings mode.  <b>CLIENT</b> CLIENT  <b>BINDINGS</b> BINDINGS
wildcardFormat	<ul style="list-style-type: none"> <li>• CHAR</li> <li>• TOPIC</li> </ul>	TOPIC	Which version of wildcard syntax is to be used.  <b>CHAR</b> CHAR  <b>TOPIC</b> TOPIC

## JMS Connection Factory (jmsConnectionFactory)

Defines a JMS connection factory configuration.

- connectionManager
- containerAuthData
- properties.wasJms
- properties.wmqJms
- recoveryAuthData

Attribute name	Data type	Default value	Description
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a connection factory.
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.
id	string		A unique configuration ID.
jndiName	string		JNDI name for a resource.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.

**connectionManager**

Connection manager for a connection factory.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.

Attribute name	Data type	Default value	Description
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

#### containerAuthData

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

### properties.wasJms

A JMS connection factory is used to create connections to the associated JMS provider of JMS destinations, for both point-to-point and publish/subscribe messaging.

false

Attribute name	Data type	Default value	Description
busName	string	defaultBus	The name of a bus when connecting to the service integration bus in a full profile server.
clientID	string	clientID	The JMS client identifier needed for durable(and for shared non-durable) topic subscriptions on all connections. This identifier is required if the application is doing durable(and for shared non-durable) publish/subscribe messaging.
durableSubscriptionHome	string	defaultME	Durable subscription home defines ME name to which connection needs to be established.
nonPersistentMapping	<ul style="list-style-type: none"> <li>• BestEffortNonPersistent</li> <li>• ReliableNonPersistent</li> <li>• ExpressNonPersistent</li> </ul>	ExpressNonPersistent	<p>The reliability applied to Non-persistent JMS messages sent using this connection factory.</p> <p><b>BestEffortNonPersistent</b> BestEffortNonPersistent</p> <p><b>ReliableNonPersistent</b> ReliableNonPersistent</p> <p><b>ExpressNonPersistent</b> ExpressNonPersistent</p>

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
persistentMapping	<ul style="list-style-type: none"> <li>AssuredPersistent</li> <li>ReliablePersistent</li> </ul>	ReliablePersistent	<p>The reliability applied to persistent JMS messages sent using this connection factory.</p> <p><b>AssuredPersistent</b> AssuredPersistent</p> <p><b>ReliablePersistent</b> ReliablePersistent</p>
readAhead	<ul style="list-style-type: none"> <li>AlwaysOff</li> <li>Default</li> <li>AlwaysOn</li> </ul>	Default	<p>Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.</p> <p><b>AlwaysOff</b> AlwaysOff</p> <p><b>Default</b> Default</p> <p><b>AlwaysOn</b> AlwaysOn</p>
remoteServerAddress	string		<p>The remote server address that has triplets separated by a comma, with the syntax hostName:portNumber:chainName, used to connect to a bootstrap server. For example, Merlin:7276:BootstrapBasicMessaging. If hostName is not specified, the default is localhost. If portNumber is not specified, the default is 7276. If chainName is not specified, the default is BootstrapBasicMessaging. Refer to the information center for more information.</p>
shareDurableSubscription	string		Controls whether or not durable subscription can be shared across connections.
targetTransportChain	string		Transport chains specify the communication protocols that can be used to communicate with the service integration bus in a full profiles server.

Attribute name	Data type	Default value	Description
temporaryQueueNamePrefix	string	temp	The prefix of up to twelve characters used for the temporary queues created by applications that use this queue connection factory.
temporaryTopicNamePrefix	string	temp	The prefix of up to twelve characters used for the temporary topics created by applications that use this topic connection factory.
userName	string		It is recommended to use a container managed authentication alias instead of configuring this property.

### properties.wmqJms

WebSphere MQ JMS connection factory

false

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	819	The coded character set identifier for a connection.
applicationName	string		The name by which an application is registered with the queue manager.
arbitraryProperties	string		Ability to specify properties not defined elsewhere
brokerCCSubQueue	string		The name of the queue from which a connection consumer receives nondurable subscription messages
brokerControlQueue	string		The name of the broker control queue
brokerPubQueue	string		The name of the queue where published messages are sent (the stream queue).
brokerQueueManager	string		The name of the queue manager on which the broker is running
brokerSubQueue	string		The name of the queue from which a nondurable message consumer receives messages
brokerVersion	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		The version of the broker being used  <b>2</b> 2 <b>1</b> 1

Attribute name	Data type	Default value	Description
ccdtURL	string		A URL that identifies the name and location of the file containing the client channel definition table (CCDT) and specifies how the file can be accessed.
channel	string		The name of the MQI channel to use.
cleanupInterval	A period of time with millisecond precision		The interval, in milliseconds, between background runs of the publish/subscribe cleanup utility. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
cleanupLevel	<ul style="list-style-type: none"> <li>• SAFE</li> <li>• FORCE</li> <li>• NONDUR</li> <li>• NONE</li> <li>• STRONG</li> </ul>	SAFE	<p>The cleanup level for a broker-based subscription store.</p> <p><b>SAFE</b> SAFE</p> <p><b>FORCE</b> FORCE</p> <p><b>NONDUR</b> NONDUR</p> <p><b>NONE</b> NONE</p> <p><b>STRONG</b> STRONG</p>
clientId	string		The client identifier for a connection
cloneSupport	<ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	DISABLED	<p>Whether two or more instances of the same durable topic subscriber can run simultaneously.</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DISABLED</b> DISABLED</p>
connectionNameList	string		A list of TCP/IP connection names (hostname(port)) used for communications. ConnectionNameList supersedes the hostname and port properties.

Attribute name	Data type	Default value	Description
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state.
headerCompression	<ul style="list-style-type: none"> <li>• SYSTEM</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing header data on a connection</p> <p><b>SYSTEM</b> SYSTEM</p> <p><b>NONE</b> NONE</p>
hostName	string		The host name or IP address of the system on which the queue manager resides. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.
localAddress	string		For a connection to a queue manager, this property specifies either or both of the following, (1) The local network interface to be used, (2) The local port, or range of local ports, to be used
messageCompression	<ul style="list-style-type: none"> <li>• RLE</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing message data on a connection.</p> <p><b>RLE</b> RLE</p> <p><b>NONE</b> NONE</p>
messageSelection	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BROKER</li> </ul>	CLIENT	<p>Determines whether message selection is done by WebSphere MQ classes for JMS or by the broker.</p> <p><b>CLIENT</b> CLIENT</p> <p><b>BROKER</b> BROKER</p>
password	Reversably encoded password (string)		The default password to use when creating a connection to the queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)

Attribute name	Data type	Default value	Description				
pollingInterval	A period of time with millisecond precision		If each message listener within a session has no suitable message on its queue, this value is the maximum interval, in milliseconds, that elapses before each message listener tries again to get a message from its queue. If it frequently happens that no suitable message is available for any of the message listeners in a session, consider increasing the value of this property. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.				
port	int Minimum: 1	1414	The port on which the queue manager listens. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.				
providerVersion	<ul style="list-style-type: none"> <li>• 7</li> <li>• 6</li> <li>• unspecified</li> </ul>	unspecified	<p>The version, release, modification level and fix pack of the queue manager to which the application intends to connect.</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50px;">7</td> <td>7</td> </tr> <tr> <td>6</td> <td>6</td> </tr> </table> <p><b>unspecified</b> unspecified</p>	7	7	6	6
7	7						
6	6						
pubAckInterval	int Minimum: 0	25	The number of messages published by a publisher before WebSphere MQ classes for JMS requests an acknowledgment from the broker				
queueManager	string		The name of the queue manager to connect to				
receiveExit	string		Identifies a channel receive exit program, or a sequence of receive exit programs to be run in succession				

Attribute name	Data type	Default value	Description
receiveExitInit	string		The user data that is passed to channel receive exit programs when they are called
rescanInterval	A period of time with millisecond precision	5s	When a message consumer in the point-to-point domain uses a message selector to select which messages it wants to receive, WebSphere MQ classes for JMS searches the WebSphere MQ queue for suitable messages in the sequence determined by the <code>MsgDeliverySequence</code> attribute of the queue. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
securityExit	string		Identifies a channel security exit program
securityExitInit	string		The user data that is passed to a channel security exit program when it is called
sendCheckCount	int Minimum: 0		The number of send calls to allow between checking for asynchronous put errors, within a single non-transacted JMS session.
sendExit	string		Identifies a channel send exit program, or a sequence of send exit programs to be run in succession.
sendExitInit	string		The user data that is passed to channel send exit programs when they are called.
shareConvAllowed	boolean	true	Whether a client connection can share its socket with other top-level JMS connections from the same process to the same queue manager, if the channel definitions match
sparseSubscriptions	boolean	false	Controls the message retrieval policy of a <code>TopicSubscriber</code> object.

Attribute name	Data type	Default value	Description
sslCertStores	string		The Lightweight Directory Access Protocol (LDAP) servers that hold certificate revocation lists (CRLs) for use on an SSL connection.
sslCipherSuite	string		The CipherSuite to use for an SSL connection.
sslFipsRequired	boolean		Whether an SSL connection must use a CipherSuite that is supported by the IBM Java JSSE FIPS provider (IBMJSSEFIPS).
sslPeerName	string		For an SSL connection, a template that is used to check the distinguished name in the digital certificate provided by the queue manager.
sslResetCount	int Minimum: 0 Maximum: 999999999	0	The total number of bytes sent and received by an SSL connection before the secret keys used by SSL are renegotiated.
statusRefreshInterval	A period of time with millisecond precision	1m	The interval, in milliseconds, between refreshes of the long running transaction that detects when a subscriber loses its connection to the queue manager. This property is relevant only if subscription store has the value QUEUE. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
subscriptionStore	<ul style="list-style-type: none"> <li>• MIGRATE</li> <li>• BROKER</li> <li>• QUEUE</li> </ul>	BROKER	<p>Determines where WebSphere MQ classes for JMS stores persistent data about active subscriptions.</p> <p><b>MIGRATE</b> MIGRATE</p> <p><b>BROKER</b> BROKER</p> <p><b>QUEUE</b> QUEUE</p>

Attribute name	Data type	Default value	Description
targetClientMatching	boolean	true	Whether a reply message, sent to the queue identified by the JMSReplyTo header field of an incoming message, has an MQRFH2 header only if the incoming message has an MQRFH2 header.
tempQPrefix	string		The prefix that is used to form the name of a WebSphere MQ dynamic queue.
tempTopicPrefix	string		When creating temporary topics, JMS generates a topic string of the form TEMP/TEMPTOPICPREFIX/unique_id, or if this property is left with the default value, just TEMP/unique_id. Specifying a non-empty TEMPTOPICPREFIX allows specific model queues to be defined for creating the managed queues for subscribers to temporary topics created under this connection.
temporaryModel	string		The name of the model queue from which JMS temporary queues are created. SYSTEM.JMS.TEMPQ.MODEL can be used by the JMS Layer to create queues which accept persistent messages, as the default value cannot. SYSTEM.DEFAULT.MODEL.QUEUE can be opened only once. SYSTEM.JMS.TEMPQ.MODEL can be opened more than once. SYSTEM.DEFAULT.MODEL.QUEUE is deprecated.
transportType	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BINDINGS</li> </ul>	CLIENT	Whether a connection to a queue manager uses client mode or bindings mode.  <b>CLIENT</b> CLIENT  <b>BINDINGS</b> BINDINGS

Attribute name	Data type	Default value	Description
userName	string		The default user name to use when creating a connection to a queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)
wildcardFormat	<ul style="list-style-type: none"> <li>• CHAR</li> <li>• TOPIC</li> </ul>	TOPIC	Which version of wildcard syntax is to be used.  <b>CHAR</b> CHAR <b>TOPIC</b> TOPIC

### recoveryAuthData

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## JMS Destination (jmsDestination)

Defines a JMS destination configuration.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
jndiName	string		JNDI name for a resource.

## JMS Queue (jmsQueue)

Defines a JMS queue configuration.

- properties.wasJms
- properties.wmqJms

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
jndiName	string		JNDI name for a resource.

### properties.wasJms

The name of the queue that this JMS queue is assigned to.

false

Attribute name	Data type	Default value	Description
deliveryMode	<ul style="list-style-type: none"><li>• NonPersistent</li><li>• Application</li><li>• Persistent</li></ul>	Application	The delivery mode for messages sent to this destination. This controls the persistence of messages on this destination.  <b>NonPersistent</b> NonPersistent <b>Application</b> Application <b>Persistent</b> Persistent
priority	int  Minimum: 0  Maximum: 9		The relative priority for messages sent to this destination, in the range 0 to 9, with 0 as the lowest priority and 9 as the highest priority.
queueName	string	Default.Queue	The name of the associated Queue
readAhead	<ul style="list-style-type: none"><li>• AlwaysOff</li><li>• AsConnection</li><li>• AlwaysOn</li></ul>	AsConnection	Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.  <b>AlwaysOff</b> AlwaysOff <b>AsConnection</b> AsConnection <b>AlwaysOn</b> AlwaysOn
timeToLive	A period of time with second precision	0s	The default time in milliseconds from its dispatch time that the system must keep the messages live in the destination. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

#### properties.wmqJms

WebSphere MQ JMS Queue

false

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	1208	The coded character set ID to be used for a connection or destination
arbitraryProperties	string		Ability to specify properties not defined elsewhere
baseQueueManagerName	string		Queue Manager name that has this queue defined on it
baseQueueName	string		Name of the Queue on the Queue Manager
encoding	string	NATIVE	How numeric data in the body of a message is represented when the message is sent to this destination. The property specifies the representation of binary integers, packed decimal integers, and floating point numbers.
expiry	string	APP	The period after which messages at a destination expire
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state
persistence	<ul style="list-style-type: none"> <li>• APP</li> <li>• QDEF</li> <li>• HIGH</li> <li>• NON</li> <li>• PERS</li> </ul>	APP	<p>The persistence of messages sent to a destination</p> <p><b>APP</b> APP</p> <p><b>QDEF</b> QDEF</p> <p><b>HIGH</b> HIGH</p> <p><b>NON</b> NON</p> <p><b>PERS</b> PERS</p>
priority	<ul style="list-style-type: none"> <li>• 3</li> <li>• 2</li> <li>• 1</li> <li>• APP</li> <li>• 0</li> <li>• 7</li> <li>• 6</li> <li>• 5</li> <li>• QDEF</li> <li>• 4</li> <li>• 9</li> <li>• 8</li> </ul>	APP	<p>The priority for messages sent to a destination</p> <p><b>3</b> 3</p> <p><b>2</b> 2</p> <p><b>1</b> 1</p> <p><b>APP</b> APP</p> <p><b>0</b> 0</p> <p><b>7</b> 7</p> <p><b>6</b> 6</p> <p><b>5</b> 5</p> <p><b>QDEF</b> QDEF</p> <p><b>4</b> 4</p> <p><b>9</b> 9</p> <p><b>8</b> 8</p>

Attribute name	Data type	Default value	Description
putAsyncAllowed	<ul style="list-style-type: none"> <li>ENABLED</li> <li>DESTINATION</li> <li>DISABLED</li> </ul>	DESTINATION	<p>Whether message producers are allowed to use asynchronous puts to send messages to this destination</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DESTINATION</b> DESTINATION</p> <p><b>DISABLED</b> DISABLED</p>
readAheadAllowed	<ul style="list-style-type: none"> <li>ENABLED</li> <li>DESTINATION</li> <li>DISABLED</li> </ul>	DESTINATION	<p>Whether the MDB is allowed to use read ahead to get nonpersistent messages from the destination into an internal buffer before receiving them</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DESTINATION</b> DESTINATION</p> <p><b>DISABLED</b> DISABLED</p>
readAheadClosePolicy	<ul style="list-style-type: none"> <li>CURRENT</li> <li>ALL</li> </ul>	ALL	<p>What happens to messages in the internal read ahead buffer when the MDB is stopped by the administrator.</p> <p><b>CURRENT</b> CURRENT</p> <p><b>ALL</b> ALL</p>
receiveCCSID	<p>int</p> <p>Minimum: 0</p>		<p>Destination property that sets the target Coded character set identifier for queue manager message conversion. The value is ignored unless receive conversion is set to WMQ_RECEIVE_CONVERSION_QMGR</p>
receiveConversion	<ul style="list-style-type: none"> <li>QMGR</li> <li>CLIENT_MSG</li> </ul>	CLIENT_MSG	<p>Destination property that determines if data conversion is going to be performed by the queue manager.</p> <p><b>QMGR</b> QMGR</p> <p><b>CLIENT_MSG</b> CLIENT_MSG</p>

Attribute name	Data type	Default value	Description
targetClient	<ul style="list-style-type: none"> <li>JMS</li> <li>MQ</li> </ul>	JMS	Whether the WebSphere MQ RFH2 format is used to exchange information with target applications  JMS    JMS MQ    MQ

## JMS Queue Connection Factory (jmsQueueConnectionFactory)

Defines a JMS queue connection factory configuration.

- connectionManager
- containerAuthData
- properties.wasJms
- properties.wmqJms
- recoveryAuthData

Attribute name	Data type	Default value	Description
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a connection factory.
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.
id	string		A unique configuration ID.
jndiName	string		JNDI name for a resource.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.

### connectionManager

Connection manager for a connection factory.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.

Attribute name	Data type	Default value	Description
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

### containerAuthData

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

### properties.wasJms

A JMS queue connection factory is used to create connections to the associated JMS provider of JMS queues, for point-to-point messaging.

false

Attribute name	Data type	Default value	Description
busName	string	defaultBus	The name of a bus when connecting to the service integration bus in a full profile server.
nonPersistentMapping	<ul style="list-style-type: none"> <li>BestEffortNonPersistent</li> <li>ReliableNonPersistent</li> <li>ExpressNonPersistent</li> </ul>	ExpressNonPersistent	<p>The reliability applied to Non-persistent JMS messages sent using this connection factory.</p> <p><b>BestEffortNonPersistent</b> BestEffortNonPersistent</p> <p><b>ReliableNonPersistent</b> ReliableNonPersistent</p> <p><b>ExpressNonPersistent</b> ExpressNonPersistent</p>
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
persistentMapping	<ul style="list-style-type: none"> <li>AssuredPersistent</li> <li>ReliablePersistent</li> </ul>	ReliablePersistent	<p>The reliability applied to persistent JMS messages sent using this connection factory.</p> <p><b>AssuredPersistent</b> AssuredPersistent</p> <p><b>ReliablePersistent</b> ReliablePersistent</p>

Attribute name	Data type	Default value	Description
readAhead	<ul style="list-style-type: none"> <li>AlwaysOff</li> <li>Default</li> <li>AlwaysOn</li> </ul>	Default	<p>Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.</p> <p><b>AlwaysOff</b> AlwaysOff</p> <p><b>Default</b> Default</p> <p><b>AlwaysOn</b> AlwaysOn</p>
remoteServerAddress	string		<p>The remote server address that has triplets separated by a comma, with the syntax <code>hostName:portNumber:chainName</code>, used to connect to a bootstrap server. For example, <code>Merlin:7276:BootstrapBasicMessaging</code>. If <code>hostName</code> is not specified, the default is <code>localhost</code>. If <code>portNumber</code> is not specified, the default is <code>7276</code>. If <code>chainName</code> is not specified, the default is <code>BootstrapBasicMessaging</code>. Refer to the information center for more information.</p>
targetTransportChain	string		<p>Transport chains specify the communication protocols that can be used to communicate with the service integration bus in a full profiles server.</p>
temporaryQueueNamePrefix	string	temp	<p>The prefix of up to twelve characters used for the temporary queues created by applications that use this queue connection factory.</p>
userName	string		<p>It is recommended to use a container managed authentication alias instead of configuring this property.</p>

#### **properties.wmqJms**

WebSphere MQ JMS queue connection factory

false

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	819	The coded character set identifier for a connection.
applicationName	string		The name by which an application is registered with the queue manager.
arbitraryProperties	string		Ability to specify properties not defined elsewhere
ccdtURL	string		A URL that identifies the name and location of the file containing the client channel definition table (CCDT) and specifies how the file can be accessed.
channel	string		The name of the MQI channel to use.
clientId	string		The client identifier for a connection.
connectionNameList	string		A list of TCP/IP connection names (hostname(port))used for communications. ConnectionNameList supersedes the hostname and port properties.
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state.
headerCompression	<ul style="list-style-type: none"> <li>• SYSTEM</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing header data on a connection</p> <p><b>SYSTEM</b> SYSTEM</p> <p><b>NONE</b> NONE</p>
hostName	string		The host name or IP address of the system on which the queue manager resides. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.
localAddress	string		For a connection to a queue manager, this property specifies either or both of the following, (1) The local network interface to be used, (2) The local port, or range of local ports, to be used

Attribute name	Data type	Default value	Description
messageCompression	<ul style="list-style-type: none"> <li>• RLE</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing message data on a connection.</p> <p><b>RLE</b> RLE <b>NONE</b> NONE</p>
password	Reversably encoded password (string)		The default password to use when creating a connection to the queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)
pollingInterval	A period of time with millisecond precision		<p>If each message listener within a session has no suitable message on its queue, this value is the maximum interval, in milliseconds, that elapses before each message listener tries again to get a message from its queue. If it frequently happens that no suitable message is available for any of the message listeners in a session, consider increasing the value of this property. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.</p>
port	<p>int</p> <p>Minimum: 1</p>	1414	The port on which the queue manager listens. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.

Attribute name	Data type	Default value	Description
providerVersion	<ul style="list-style-type: none"> <li>• 7</li> <li>• 6</li> <li>• unspecified</li> </ul>	unspecified	<p>The version, release, modification level and fix pack of the queue manager to which the application intends to connect.</p> <p>7        7</p> <p>6        6</p> <p><b>unspecified</b> unspecified</p>
queueManager	string		The name of the queue manager to connect to
receiveExit	string		Identifies a channel receive exit program, or a sequence of receive exit programs to be run in succession
receiveExitInit	string		The user data that is passed to channel receive exit programs when they are called
rescanInterval	A period of time with millisecond precision	5s	<p>When a message consumer in the point-to-point domain uses a message selector to select which messages it wants to receive, WebSphere MQ classes for JMS searches the WebSphere MQ queue for suitable messages in the sequence determined by the <code>MsgDeliverySequence</code> attribute of the queue. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.</p>
securityExit	string		Identifies a channel security exit program
securityExitInit	string		The user data that is passed to a channel security exit program when it is called
sendCheckCount	int Minimum: 0		The number of send calls to allow between checking for asynchronous put errors, within a single non-transacted JMS session.

Attribute name	Data type	Default value	Description
sendExit	string		Identifies a channel send exit program, or a sequence of send exit programs to be run in succession.
sendExitInit	string		The user data that is passed to channel send exit programs when they are called.
shareConvAllowed	boolean	true	Whether a client connection can share its socket with other top-level JMS connections from the same process to the same queue manager, if the channel definitions match
sslCertStores	string		The Lightweight Directory Access Protocol (LDAP) servers that hold certificate revocation lists (CRLs) for use on an SSL connection.
sslCipherSuite	string		The CipherSuite to use for an SSL connection.
sslFipsRequired	boolean		Whether an SSL connection must use a CipherSuite that is supported by the IBM Java JSSE FIPS provider (IBMJSEFIPS).
sslPeerName	string		For an SSL connection, a template that is used to check the distinguished name in the digital certificate provided by the queue manager.
sslResetCount	int Minimum: 0 Maximum: 999999999		The total number of bytes sent and received by an SSL connection before the secret keys used by SSL are renegotiated.
targetClientMatching	boolean	true	Whether a reply message, sent to the queue identified by the JMSReplyTo header field of an incoming message, has an MQRFH2 header only if the incoming message has an MQRFH2 header.
tempQPrefix	string		The prefix that is used to form the name of a WebSphere MQ dynamic queue.

Attribute name	Data type	Default value	Description
temporaryModel	string		The name of the model queue from which JMS temporary queues are created. SYSTEM.JMS.TEMPQ.MODEL can be used by the JMS Layer to create queues which accept persistent messages, as the default value cannot. SYSTEM.DEFAULT.MODEL.QUEUE can be opened only once. SYSTEM.JMS.TEMPQ.MODEL can be opened more than once. SYSTEM.DEFAULT.MODEL.QUEUE is deprecated.
transportType	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BINDINGS</li> </ul>	CLIENT	Whether a connection to a queue manager uses client mode or bindings mode.  <b>CLIENT</b> CLIENT  <b>BINDINGS</b> BINDINGS
userName	string		The default user name to use when creating a connection to a queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)

### recoveryAuthData

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## JMS Topic (jmsTopic)

Defines a JMS topic configuration.

- properties.wasJms
- properties.wmqJms

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
jndiName	string		JNDI name for a resource.

### properties.wasJms

The name of the topic that this JMS topic is assigned to, in the topic space defined by the Topic space property.

false

Attribute name	Data type	Default value	Description
deliveryMode	<ul style="list-style-type: none"> <li>• NonPersistent</li> <li>• Application</li> <li>• Persistent</li> </ul>	Application	<p>The delivery mode for messages sent to this destination. This controls the persistence of messages on this destination.</p> <p><b>NonPersistent</b> NonPersistent</p> <p><b>Application</b> Application</p> <p><b>Persistent</b> Persistent</p>
priority	<p>int</p> <p>Minimum: 0</p> <p>Maximum: 9</p>		<p>The relative priority for messages sent to this destination, in the range 0 to 9, with 0 as the lowest priority and 9 as the highest priority.</p>
readAhead	<ul style="list-style-type: none"> <li>• AlwaysOff</li> <li>• AsConnection</li> <li>• AlwaysOn</li> </ul>	AsConnection	<p>Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.</p> <p><b>AlwaysOff</b> AlwaysOff</p> <p><b>AsConnection</b> AsConnection</p> <p><b>AlwaysOn</b> AlwaysOn</p>

Attribute name	Data type	Default value	Description
timeToLive	A period of time with second precision	0s	The default time in milliseconds from its dispatch time that the system must keep the messages live in the destination. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
topicName	string	Default.Topic	The name of the topic that this JMS topic is assigned to, in the topic space defined by the Topic space property.
topicSpace	string	Default.Topic.Space	A topic space is a location for publish/subscribe messaging.

#### properties.wmqJms

WebSphere MQ JMS Topic

false

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	1208	The coded character set ID to be used for a connection or destination
arbitraryProperties	string		Ability to specify properties not defined elsewhere
baseTopicName	string		Topic string to open
brokerCCDurSubQueue	string	SYSTEM.JMS.D.CC.SUBSCRIBER.QUEUE	The name of the queue from which non-durable subscription messages are retrieved for a connection consumer
brokerDurSubQueue	string	SYSTEM.JMS.D.SUBSCRIBER.QUEUE	The name of the queue from which durable subscription messages are retrieved
brokerPubQueue	string		The name of the queue where published messages are sent (the stream queue)
brokerPubQueueManager	string		The name of the queue manager that owns the queue where messages published on the topic are sent

Attribute name	Data type	Default value	Description
brokerVersion	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>	1	<p>The version of the broker being used</p> <p><b>2</b>     2</p> <p><b>1</b>     1</p>
encoding	string	NATIVE	How numeric data in the body of a message is represented when the message is sent to this destination. The property specifies the representation of binary integers, packed decimal integers, and floating point numbers.
expiry	string	APP	The period after which messages at a destination expire
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state
persistence	<ul style="list-style-type: none"> <li>• APP</li> <li>• QDEF</li> <li>• HIGH</li> <li>• NON</li> <li>• PERS</li> </ul>	APP	<p>The persistence of messages sent to a destination</p> <p><b>APP</b>    APP</p> <p><b>QDEF</b>   QDEF</p> <p><b>HIGH</b>   HIGH</p> <p><b>NON</b>    NON</p> <p><b>PERS</b>   PERS</p>
priority	<ul style="list-style-type: none"> <li>• 3</li> <li>• 2</li> <li>• 1</li> <li>• APP</li> <li>• 0</li> <li>• 7</li> <li>• 6</li> <li>• 5</li> <li>• QDEF</li> <li>• 4</li> <li>• 9</li> <li>• 8</li> </ul>	APP	<p>The priority for messages sent to a destination</p> <p><b>3</b>     3</p> <p><b>2</b>     2</p> <p><b>1</b>     1</p> <p><b>APP</b>   APP</p> <p><b>0</b>     0</p> <p><b>7</b>     7</p> <p><b>6</b>     6</p> <p><b>5</b>     5</p> <p><b>QDEF</b>   QDEF</p> <p><b>4</b>     4</p> <p><b>9</b>     9</p> <p><b>8</b>     8</p>

Attribute name	Data type	Default value	Description
putAsyncAllowed	<ul style="list-style-type: none"> <li>ENABLED</li> <li>DESTINATION</li> <li>DISABLED</li> </ul>	DESTINATION	<p>Whether message producers are allowed to use asynchronous puts to send messages to this destination</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DESTINATION</b> DESTINATION</p> <p><b>DISABLED</b> DISABLED</p>
readAheadAllowed	<ul style="list-style-type: none"> <li>ENABLED</li> <li>DESTINATION</li> <li>DISABLED</li> </ul>	DESTINATION	<p>Whether the MDB is allowed to use read ahead to get nonpersistent messages from the destination into an internal buffer before receiving them</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DESTINATION</b> DESTINATION</p> <p><b>DISABLED</b> DISABLED</p>
readAheadClosePolicy	<ul style="list-style-type: none"> <li>CURRENT</li> <li>ALL</li> </ul>	ALL	<p>What happens to messages in the internal read ahead buffer when the MDB is stopped by the administrator.</p> <p><b>CURRENT</b> CURRENT</p> <p><b>ALL</b> ALL</p>
receiveCCSID	<p>int</p> <p>Minimum: 0</p>		<p>Destination property that sets the target Coded character set identifier for queue manager message conversion. The value is ignored unless receive conversion is set to WMQ_RECEIVE_CONVERSION_QMGR</p>
receiveConversion	<ul style="list-style-type: none"> <li>QMGR</li> <li>CLIENT_MSG</li> </ul>	CLIENT_MSG	<p>Destination property that determines if data conversion is going to be performed by the queue manager.</p> <p><b>QMGR</b> QMGR</p> <p><b>CLIENT_MSG</b> CLIENT_MSG</p>

Attribute name	Data type	Default value	Description
targetClient	<ul style="list-style-type: none"> <li>JMS</li> <li>MQ</li> </ul>	JMS	Whether the WebSphere MQ RFH2 format is used to exchange information with target applications  JMS    JMS MQ    MQ

## JMS Topic Connection Factory (jmsTopicConnectionFactory)

Defines a JMS topic connection factory configuration.

- connectionManager
- containerAuthData
- properties.wasJms
- properties.wmqJms
- recoveryAuthData

Attribute name	Data type	Default value	Description
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a connection factory.
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.
id	string		A unique configuration ID.
jndiName	string		JNDI name for a resource.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.

### connectionManager

Connection manager for a connection factory.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.

Attribute name	Data type	Default value	Description
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

#### containerAuthData

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

### properties.wasJms

A JMS topic connection factory is used to create connections to the associated JMS provider of JMS destinations, for publish/subscribe messaging.

false

Attribute name	Data type	Default value	Description
busName	string	defaultBus	The name of a bus when connecting to the service integration bus in a full profile server.
clientID	string	clientID	The JMS client identifier needed for durable(and for shared non-durable) topic subscriptions on all connections. This identifier is required if the application is doing durable(and for shared non-durable) publish/subscribe messaging.
durableSubscriptionHome	string	defaultME	Durable subscription home defines ME name to which connection needs to be established.
nonPersistentMapping	<ul style="list-style-type: none"> <li>• BestEffortNonPersistent</li> <li>• ReliableNonPersistent</li> <li>• ExpressNonPersistent</li> </ul>	ExpressNonPersistent	<p>The reliability applied to Non-persistent JMS messages sent using this connection factory.</p> <p><b>BestEffortNonPersistent</b> BestEffortNonPersistent</p> <p><b>ReliableNonPersistent</b> ReliableNonPersistent</p> <p><b>ExpressNonPersistent</b> ExpressNonPersistent</p>

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
persistentMapping	<ul style="list-style-type: none"> <li>AssuredPersistent</li> <li>ReliablePersistent</li> </ul>	ReliablePersistent	<p>The reliability applied to persistent JMS messages sent using this connection factory.</p> <p><b>AssuredPersistent</b> AssuredPersistent</p> <p><b>ReliablePersistent</b> ReliablePersistent</p>
readAhead	<ul style="list-style-type: none"> <li>AlwaysOff</li> <li>Default</li> <li>AlwaysOn</li> </ul>	Default	<p>Read ahead is an optimization that preemptively assigns messages to consumers. This processes the consumer requests faster.</p> <p><b>AlwaysOff</b> AlwaysOff</p> <p><b>Default</b> Default</p> <p><b>AlwaysOn</b> AlwaysOn</p>
remoteServerAddress	string		<p>The remote server address that has triplets separated by a comma, with the syntax hostName:portNumber:chainName, used to connect to a bootstrap server. For example, Merlin:7276:BootstrapBasicMessaging. If hostName is not specified, the default is localhost. If portNumber is not specified, the default is 7276. If chainName is not specified, the default is BootstrapBasicMessaging. Refer to the information center for more information.</p>
shareDurableSubscription	string		Controls whether or not durable subscription can be shared across connections.
targetTransportChain	string		Transport chains specify the communication protocols that can be used to communicate with the service integration bus in a full profiles server.

Attribute name	Data type	Default value	Description
temporaryTopicNamePrefix	string	temp	The prefix of up to twelve characters used for the temporary topics created by applications that use this topic connection factory.
userName	string		It is recommended to use a container managed authentication alias instead of configuring this property.

### properties.wmqJms

WebSphere MQ JMS topic connection factory

false

Attribute name	Data type	Default value	Description
CCSID	int Minimum: 1	819	The coded character set identifier for a connection.
applicationName	string		The name by which an application is registered with the queue manager.
arbitraryProperties	string		Ability to specify properties not defined elsewhere
brokerCCSubQueue	string		The name of the queue from which a connection consumer receives nondurable subscription messages
brokerControlQueue	string		The name of the broker control queue
brokerPubQueue	string		The name of the queue where published messages are sent (the stream queue).
brokerQueueManager	string		The name of the queue manager on which the broker is running
brokerSubQueue	string		The name of the queue from which a nondurable message consumer receives messages
brokerVersion	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		The version of the broker being used  2        2 1        1
ccdtURL	string		A URL that identifies the name and location of the file containing the client channel definition table (CCDT) and specifies how the file can be accessed.

Attribute name	Data type	Default value	Description
channel	string		The name of the MQI channel to use.
cleanupInterval	A period of time with millisecond precision		The interval, in milliseconds, between background runs of the publish/subscribe cleanup utility. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
cleanupLevel	<ul style="list-style-type: none"> <li>• SAFE</li> <li>• FORCE</li> <li>• NONDUR</li> <li>• NONE</li> <li>• STRONG</li> </ul>	SAFE	<p>The cleanup level for a broker-based subscription store.</p> <p><b>SAFE</b> SAFE</p> <p><b>FORCE</b> FORCE</p> <p><b>NONDUR</b> NONDUR</p> <p><b>NONE</b> NONE</p> <p><b>STRONG</b> STRONG</p>
clientId	string		The client identifier for a connection
cloneSupport	<ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	DISABLED	<p>Whether two or more instances of the same durable topic subscriber can run simultaneously.</p> <p><b>ENABLED</b> ENABLED</p> <p><b>DISABLED</b> DISABLED</p>
connectionNameList	string		A list of TCP/IP connection names (hostname(port)) used for communications. ConnectionNameList supersedes the hostname and port properties.
failIfQuiesce	boolean	true	Whether calls to certain methods fail if the queue manager is in a quiescing state.

Attribute name	Data type	Default value	Description
headerCompression	<ul style="list-style-type: none"> <li>• SYSTEM</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing header data on a connection</p> <p><b>SYSTEM</b> SYSTEM</p> <p><b>NONE</b> NONE</p>
hostName	string		<p>The host name or IP address of the system on which the queue manager resides. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.</p>
localAddress	string		<p>For a connection to a queue manager, this property specifies either or both of the following, (1) The local network interface to be used, (2) The local port, or range of local ports, to be used</p>
messageCompression	<ul style="list-style-type: none"> <li>• RLE</li> <li>• NONE</li> </ul>	NONE	<p>A list of the techniques that can be used for compressing message data on a connection.</p> <p><b>RLE</b> RLE</p> <p><b>NONE</b> NONE</p>
messageSelection	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BROKER</li> </ul>	CLIENT	<p>Determines whether message selection is done by WebSphere MQ classes for JMS or by the broker.</p> <p><b>CLIENT</b> CLIENT</p> <p><b>BROKER</b> BROKER</p>
password	Reversably encoded password (string)		<p>The default password to use when creating a connection to the queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)</p>

Attribute name	Data type	Default value	Description						
pollingInterval	A period of time with millisecond precision		If each message listener within a session has no suitable message on its queue, this value is the maximum interval, in milliseconds, that elapses before each message listener tries again to get a message from its queue. If it frequently happens that no suitable message is available for any of the message listeners in a session, consider increasing the value of this property. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.						
port	int Minimum: 1	1414	The port on which the queue manager listens. The hostname and port properties are superseded by the ConnectionNameList property when it is specified.						
providerVersion	<ul style="list-style-type: none"> <li>• 7</li> <li>• 6</li> <li>• unspecified</li> </ul>	unspecified	<p>The version, release, modification level and fix pack of the queue manager to which the application intends to connect.</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50px;">7</td> <td>7</td> </tr> <tr> <td>6</td> <td>6</td> </tr> <tr> <td><b>unspecified</b></td> <td><b>unspecified</b></td> </tr> </table>	7	7	6	6	<b>unspecified</b>	<b>unspecified</b>
7	7								
6	6								
<b>unspecified</b>	<b>unspecified</b>								
pubAckInterval	int Minimum: 0	25	The number of messages published by a publisher before WebSphere MQ classes for JMS requests an acknowledgment from the broker						
queueManager	string		The name of the queue manager to connect to						
receiveExit	string		Identifies a channel receive exit program, or a sequence of receive exit programs to be run in succession						

Attribute name	Data type	Default value	Description
receiveExitInit	string		The user data that is passed to channel receive exit programs when they are called
rescanInterval	A period of time with millisecond precision	5s	When a message consumer in the point-to-point domain uses a message selector to select which messages it wants to receive, WebSphere MQ classes for JMS searches the WebSphere MQ queue for suitable messages in the sequence determined by the <code>MsgDeliverySequence</code> attribute of the queue. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
securityExit	string		Identifies a channel security exit program
securityExitInit	string		The user data that is passed to a channel security exit program when it is called
sendCheckCount	int Minimum: 0		The number of send calls to allow between checking for asynchronous put errors, within a single non-transacted JMS session.
sendExit	string		Identifies a channel send exit program, or a sequence of send exit programs to be run in succession.
sendExitInit	string		The user data that is passed to channel send exit programs when they are called.
shareConvAllowed	boolean	true	Whether a client connection can share its socket with other top-level JMS connections from the same process to the same queue manager, if the channel definitions match
sparseSubscriptions	boolean	false	Controls the message retrieval policy of a <code>TopicSubscriber</code> object.

Attribute name	Data type	Default value	Description
sslCertStores	string		The Lightweight Directory Access Protocol (LDAP) servers that hold certificate revocation lists (CRLs) for use on an SSL connection.
sslCipherSuite	string		The CipherSuite to use for an SSL connection.
sslFipsRequired	boolean		Whether an SSL connection must use a CipherSuite that is supported by the IBM Java JSSE FIPS provider (IBMJSSEFIPS).
sslPeerName	string		For an SSL connection, a template that is used to check the distinguished name in the digital certificate provided by the queue manager.
sslResetCount	int Minimum: 0 Maximum: 999999999	0	The total number of bytes sent and received by an SSL connection before the secret keys used by SSL are renegotiated.
statusRefreshInterval	A period of time with millisecond precision	1m	The interval, in milliseconds, between refreshes of the long running transaction that detects when a subscriber loses its connection to the queue manager. This property is relevant only if subscription store has the value QUEUE. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
subscriptionStore	<ul style="list-style-type: none"> <li>• MIGRATE</li> <li>• BROKER</li> <li>• QUEUE</li> </ul>	BROKER	<p>Determines where WebSphere MQ classes for JMS stores persistent data about active subscriptions.</p> <p><b>MIGRATE</b> MIGRATE</p> <p><b>BROKER</b> BROKER</p> <p><b>QUEUE</b> QUEUE</p>

Attribute name	Data type	Default value	Description
targetClientMatching	boolean	true	Whether a reply message, sent to the queue identified by the JMSReplyTo header field of an incoming message, has an MQRFH2 header only if the incoming message has an MQRFH2 header.
tempTopicPrefix	string		When creating temporary topics, JMS generates a topic string of the form TEMP/TEMPTOPICPREFIX/unique_id, or if this property is left with the default value, just TEMP/unique_id. Specifying a non-empty TEMPTOPICPREFIX allows specific model queues to be defined for creating the managed queues for subscribers to temporary topics created under this connection.
transportType	<ul style="list-style-type: none"> <li>• CLIENT</li> <li>• BINDINGS</li> </ul>	CLIENT	Whether a connection to a queue manager uses client mode or bindings mode.  <b>CLIENT</b> CLIENT <b>BINDINGS</b> BINDINGS
userName	string		The default user name to use when creating a connection to a queue manager. (It is recommended to use a container managed authentication alias instead of configuring this property)
wildcardFormat	<ul style="list-style-type: none"> <li>• CHAR</li> <li>• TOPIC</li> </ul>	TOPIC	Which version of wildcard syntax is to be used.  <b>CHAR</b> CHAR <b>TOPIC</b> TOPIC

**recoveryAuthData**

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## JNDI Entry (jndiEntry)

A single entry in the JNDI default namespace.

Attribute name	Data type	Default value	Description
decode	boolean	false	True if value needs to be decoded on lookup.
id	string		A unique configuration ID.
jndiName	string		The JNDI name to use for this entry.
value	string		The JNDI value to associate with the name.

## JNDI Object Factory (jndiObjectFactory)

ObjectFactory to be used by a JNDI Reference entry.

- library
  - file
  - fileset
  - folder

Attribute name	Data type	Default value	Description
className	string		ObjectFactory implementation class name.
id	string		A unique configuration ID.
libraryRef	A reference to top level library element (string).		Library containing the factory implementation class.
objectClassName	string	java.lang.Object	Type of object returned from the factory.

### library

Library containing the factory implementation class.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

### library > file

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

### library > fileset

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

## JNDI Reference Entry (jndiReferenceEntry)

Reference entry in the JNDI default namespace.

- factory
  - library
  - file
  - fileset
  - folder
- properties

Attribute name	Data type	Default value	Description
decode	boolean	false	True if value needs to be decoded on lookup.
factoryRef	A reference to top level jndiObjectFactory element (string).		Object factory for the reference entry.
id	string		A unique configuration ID.
jndiName	string		JNDI name for the reference entry.

**factory**

Object factory for the reference entry.

false

Attribute name	Data type	Default value	Description
className	string		ObjectFactory implementation class name.
libraryRef	A reference to top level library element (string).		Library containing the factory implementation class.
objectClassName	string	java.lang.Object	Type of object returned from the factory.

#### **factory > library**

Library containing the factory implementation class.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

#### **factory > library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

#### **factory > library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.

Attribute name	Data type	Default value	Description
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

#### **factory > library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

#### **properties**

The properties for the reference entry.

false

## **JNDI URL Entry (jndiURLEntry)**

A single entry in the JNDI default namespace that is used for binding java.net.URL entries.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
jndiName	string		The JNDI name to use for this entry.

Attribute name	Data type	Default value	Description
value	string		The JNDI URL value to associate with the name.

## JPA Container (jpa)

Configuration properties for the Java Persistence API container.

- excludedApplication

Attribute name	Data type	Default value	Description
defaultJtaDataSourceJndiName	string		Default Java™ Transaction API (JTA) data source JNDI name to be used by applications running in this server. By default, data sources are JTA. Only data sources that are transactional are allowed in this field.
defaultNonJtaDataSourceJndiName	string		Default non-transactional data source JNDI name to be used by applications running in this server. Only data sources that have been marked as non-transactional are allowed in this field.
defaultPersistenceProvider	string		Default persistence provider class name. If this property is not specified, the default provider is dependent on which JPA feature is enabled.
entityManagerPoolCapacity	int	-1	EntityManager pool capacity per PersistenceContext reference. The minimum is 0 and the maximum is 500.

Attribute name	Data type	Default value	Description
ignoreDataSourceErrors	boolean		If true, errors that occur while attempting to lookup a data source specified by the <jta-data-source> or <non-jta-data-source> elements in the persistence.xml file are reported and ignored, which allows the persistence provider to determine a default data source. If false, the errors are propagated to the persistence provider so that the errors can be diagnosed more easily, but misconfigured applications might not work. By default, this property is true if JPA 2.0 is enabled and false otherwise.

#### excludedApplication

An application to be excluded from JPA processing.

false

string

## JSP Engine (jspEngine)

JSP 2.2 configuration

Attribute name	Data type	Default value	Description
disableJspRuntimeCompilation	boolean	false	Disable compilation of JSPs at runtime.
disableResourceInjection	boolean	false	Disable injection of resources into JSPs.
extendedDocumentRoot	string		Directory that the JSP engine will search for additional JSP files to serve.
jdkSourceLevel	<ul style="list-style-type: none"> <li>• 17</li> <li>• 18</li> <li>• 15</li> <li>• 16</li> <li>• 13</li> <li>• 14</li> </ul>	15	Default Java source level for JSPs compiled by the JSP engine. <b>17</b> 17 <b>18</b> 18 <b>15</b> 15 <b>16</b> 16 <b>13</b> 13 <b>14</b> 14
keepGenerated	boolean	false	Keep Java source files generated for JSPs.

Attribute name	Data type	Default value	Description
prepareJSPs	int		When this attribute is present, all JSPs larger than the value (in kilobytes) are compiled at application server startup. Set this to 0 to compile all JSPs.
recompileJspOnRestart	boolean	false	Recompile JSPs after an application is restarted. JSPs are recompiled on first access.
scratchdir	string		When this attribute is set, the JSPs are compiled to the specified directory instead of the server workarea directory.
useImplicitTagLibs	boolean	true	Allow JSPs to use jsx and tsx tag libs.
useInMemory	boolean	false	Generate Java source and classes in memory (without writing to disk).

## Keystore (keyStore)

A repository of security certificates used for SSL encryption.

- keyEntry

Attribute name	Data type	Default value	Description
fileBased	boolean	true	Specify true if the keystore is file based and false if the keystore is a SAF keyring or hardware keystore type.
id	string		A unique configuration ID.
location	A file, directory or url.	\${server.output.dir}/resources/security/key.jks	An absolute or relative path to the keystore file. If a relative path is provided, the server will attempt to locate the file in the \${server.config.dir}/resources/security directory. Use the keystore file for a file-based keystore, the keyring name for SAF keyrings, or the device configuration file for hardware cryptography devices. In the SSL minimal configuration, the location of the file is assumed to be \${server.config.dir}/resources/security/key.jks.

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		The password used to load the keystore file. The value can be stored in clear text or encoded form. Use the securityUtility tool to encode the password.
pollingRate	A period of time with millisecond precision	500ms	Rate at which the server checks for updates to a keystore file. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
readOnly	boolean	false	Specify true if the keystore is to be used by the server for reading and false if write operations will be performed by the server on the keystore.
type	string	jks	A keystore type supported by the target SDK.

Attribute name	Data type	Default value	Description
updateTrigger	<ul style="list-style-type: none"> <li>• mbean</li> <li>• polled</li> <li>• disabled</li> </ul>	mbean	<p>Keystore file update method or trigger.</p> <p><b>mbean</b> Server will only update the keystore when prompted by the FileNotificationMbean. The FileNotificationMbean is typically called by an external program such as an integrated development environment or a management application.</p> <p><b>polled</b> Server will scan for keystore file changes at the polling interval and update if the keystore file has detectable changes.</p> <p><b>disabled</b> Disables all update monitoring. Changes to the keystore file will not be applied while the server is running.</p>

### keyEntry

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
keyPassword	Reversably encoded password (string)		Password of the private key entry in the keystore.
name	string		Name of the private key entry in the keystore.

## LDAP User Registry (IdapRegistry)

Configuration properties for the LDAP user registry.

- activedFilters
- attributeConfiguration
  - attribute
  - externalIdAttribute
- contextPool

- customFilters
- domino50Filters
- edirectoryFilters
- failoverServers
  - server
- idsFilters
- iplanetFilters
- ldapCache
  - attributesCache
  - searchResultsCache
- ldapEntityType
  - objectClass
  - searchBase
- netscapeFilters
- securewayFilters

Attribute name	Data type	Default value	Description
activatedFiltersRef	A reference to top level activatedLdapFilterProperties element (string).		Specifies the list of default Microsoft Active Directory LDAP filters.
baseDN	string		Base distinguished name (DN) of the directory service, which indicates the starting point for LDAP searches in the directory service.
bindDN	string		Distinguished name (DN) for the application server, which is used to bind to the directory service.
bindPassword	Reversably encoded password (string)		Password for the bind DN. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
certificateFilter	string		Specifies the filter certificate mapping property for the LDAP filter. The filter is used to map attributes in the client certificate to entries in the LDAP registry. For example, the filter can be specified as: uid=\${SubjectCN}.

Attribute name	Data type	Default value	Description
certificateMapMode	<ul style="list-style-type: none"> <li>EXACT_DN</li> <li>CERTIFICATE_FILTER</li> </ul>		<p>Specifies whether to map x.509 certificates into an LDAP directory by EXACT_DN or CERTIFICATE_FILTER. Specify CERTIFICATE_FILTER to use the specified certificate filter for the mapping.</p> <p><b>EXACT_DN</b> exactDN</p> <p><b>CERTIFICATE_FILTER</b> certFilter</p>
connectTimeout	A period of time with millisecond precision	1m	<p>Maximum time for establishing a connection to the LDAP server. An error message will be logged if the specified time expires. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.</p>
customFiltersRef	A reference to top level customLdapFilterProperties element (string).		Specifies the list of default Custom LDAP filters.
domino50FiltersRef	A reference to top level domino50LdapFilterProperties element (string).		Specifies the list of default IBM Lotus Domino LDAP filters.
edirectoryFiltersRef	A reference to top level edirectoryLdapFilterProperties element (string).		Specifies the list of Novell eDirectory LDAP filters.
host	string		Address of the LDAP server in the form of an IP address or a domain name service (DNS) name.
id	string		A unique configuration ID.
idsFiltersRef	A reference to top level idsLdapFilterProperties element (string).		Specifies the list of default IBM Tivoli Directory Server LDAP filters.
ignoreCase	boolean	true	Perform a case-insensitive authentication check.
iplanetFiltersRef	A reference to top level iplanetLdapFilterProperties element (string).		Specifies the list of default Sun Java System Directory Server LDAP filters.

Attribute name	Data type	Default value	Description
ldapType	<ul style="list-style-type: none"> <li>• Sun Java System Directory Server</li> <li>• Netscape Directory Server</li> <li>• Microsoft Active Directory</li> <li>• IBM Tivoli Directory Server</li> <li>• IBM Lotus Domino</li> <li>• Custom</li> <li>• IBM SecureWay Directory Server</li> <li>• Novell eDirectory</li> </ul>		<p>Type of LDAP server to which a connection will be established.</p> <p><b>Sun Java System Directory Server</b> iplanet</p> <p><b>Netscape Directory Server</b> netscape</p> <p><b>Microsoft Active Directory</b> actived</p> <p><b>IBM Tivoli Directory Server</b> ibm_dir_server</p> <p><b>IBM Lotus Domino</b> domino50</p> <p><b>Custom</b> custom</p> <p><b>IBM SecureWay Directory Server</b> secureway</p> <p><b>Novell eDirectory</b> edirectory</p>
netscapeFiltersRef	A reference to top level netscapeLdapFilterProperties element (string).		Specifies the list of default Netscape Directory Server LDAP filters.
port	int		Port number of the LDAP server.
realm	string	LdapRegistry	The realm name that represents the user registry.
recursiveSearch	boolean	false	Performs a nested group search. Select this option only if the LDAP server does not support recursive server-side searches.
returnToPrimaryServer	boolean	true	A boolean value that indicates if the search should be done against the Primary Server.
reuseConnection	boolean	true	Requests the application server to reuse the LDAP server connection.

Attribute name	Data type	Default value	Description
searchTimeout	A period of time with millisecond precision	1m	Maximum time for an LDAP server to respond before a request is canceled. This is equivalent to a read timeout once the connection is established. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
securewayFiltersRef	A reference to top level securewayLdapFilterProperties element (string).		Specifies the list of default IBM SecureWay Directory Server LDAP filters.
sslEnabled	boolean	false	Indicates whether an SSL connection should be made to the LDAP server.
sslRef	A reference to top level ssl element (string).		ID of the SSL configuration to be used to connect to the SSL-enabled LDAP server.

#### activatedFilters

Specifies the list of default Microsoft Active Directory LDAP filters.

false

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(objectcategory=group))	An LDAP filter clause for searching the user registry for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	memberOf:member	An LDAP filter that identifies user to group memberships.
userFilter	string	(&(sAMAccountName=%v)(objectcategory=user))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	user:sAMAccountName	An LDAP filter that maps the name of a user to an LDAP entry.

#### attributeConfiguration

The configuration that maps the LDAP attributes with the user registry schema (for example; Person, PersonAccount or Group) field names.

false

**attributeConfiguration > attribute**

Define the user registry schema field names to be mapped to the LDAP attribute.

false

Attribute name	Data type	Default value	Description
defaultValue	string		The default value of the attribute.
entityType	string		The entity type of the attribute.
id	string		A unique configuration ID.
name	string		The name of the LDAP attribute.
propertyName	string		The user registry schema field name that needs to be mapped with the LDAP attribute.
syntax	string		The attribute syntax.

**attributeConfiguration > externalIdAttribute**

Define the name of the LDAP attribute and its properties that needs to be mapped to the user registry externalId attribute.

false

Attribute name	Data type	Default value	Description
autoGenerate	boolean	false	When enabled, the externalId attribute value is generated automatically by the user registry instead of using the value that is stored in LDAP. By default it is disabled.
entityType	string		The entity type of the attribute.
id	string		A unique configuration ID.
name	string		The name of the LDAP attribute to be used for the user registry externalId attribute.
syntax	string		The attribute syntax.

**contextPool**

Properties of the context pool.

false

Attribute name	Data type	Default value	Description
enabled	boolean	true	A boolean value that determines if the context pool is enabled. Disabling it can cause performance degradation.

Attribute name	Data type	Default value	Description
initialSize	int	1	An integer value that determines the initial size of the context pool. Set this based on the load on the repository.
maxSize	int	0	An integer value that defines the maximum context pool size. Set this based on the maximum load on the repository.
preferredSize	int	3	The preferred size of the context pool. Set this based on the load on the repository.
timeout	A period of time with millisecond precision	0s	The duration after which the context pool times out. An integer that represents the time that an idle context instance can remain in the pool without being closed and removed from the pool. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
waitTime	A period of time with millisecond precision	3s	The duration after which the context pool times out. The time interval that the request waits until the context pool checks again if an idle context instance is available in the pool when the number of context instances reaches the maximum pool size. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

#### customFilters

Specifies the list of default Custom LDAP filters.

false

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(!(objectclass=groupOfNames)(!(objectclass=groupOfUniqueNames)(objectclass=groupOfDynamicNames)))	An LDAP filter clause for searching the user registry for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	ibm-allGroups:member;ibm-allGroups:uniqueMember;groupOfNames:member;groupOfUniqueNames:member	An LDAP filter that identifies user to group memberships.
userFilter	string	(&(uid=%v)(objectclass=ePerson))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	*:uid	An LDAP filter that maps the name of a user to an LDAP entry.

### domino50Filters

Specifies the list of default IBM Lotus Domino LDAP filters.

false

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(objectclass=dominoGroup))	An LDAP filter clause for searching the user registry for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	dominoGroup:member	An LDAP filter that identifies user to group memberships.
userFilter	string	(&(uid=%v)(objectclass=Person))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	person:uid	An LDAP filter that maps the name of a user to an LDAP entry.

### edirectoryFilters

Specifies the list of Novell eDirectory LDAP filters.

false

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(objectclass=groupOfNames))	An LDAP filter clause for searching the user registry for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.

Attribute name	Data type	Default value	Description
groupMemberIdMap	string	groupOfNames:member	An LDAP filter that identifies user to group memberships.
userFilter	string	(&(cn=%v)(objectclass=Person))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	person:cn	An LDAP filter that maps the name of a user to an LDAP entry.

### failoverServers

List of LDAP failover servers.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Configuration properties for LDAP failover servers. Specify it as a backup server for the primary LDAP servers. For example, <pre>&lt;failoverServers name="failoverLdapServers"&gt;&lt;server host="myfullyqualifiedhostname1" port="389"/&gt;&lt;server host="myfullyqualifiedhostname2" port="389"/&gt;&lt;/failoverServers&gt;</pre>

### failoverServers > server

Configuration properties for LDAP failover server.

false

Attribute name	Data type	Default value	Description
host	string		LDAP server host name, which can be either an IP address or a domain name service (DNS) name.
id	string		A unique configuration ID.
port	int		LDAP failover server port.

### idsFilters

Specifies the list of default IBM Tivoli Directory Server LDAP filters.

false

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(!(objectclass=groupOfNames)(objectclass=groupOfUniqueNames)(objectclass=groupOfNames))	An LDAP filter clause for searching the user registry for groups.

Attribute name	Data type	Default value	Description
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	ibm-allGroups:member;ibm-allGroups:uniqueMember;groupOfNames:uniqueMember;groupOfUniqueNames:uniqueMember	An LDAP filter that identifies user to group memberships.
userFilter	string	(&(uid=%v)(objectclass=ePerson))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	*:uid	An LDAP filter that maps the name of a user to an LDAP entry.

### iplanetFilters

Specifies the list of default Sun Java System Directory Server LDAP filters.

false

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(objectclass=ldapsubentry))	An LDAP filter clause for searching the user registry for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	nsRole:nsRole	An LDAP filter that identifies user to group memberships.
userFilter	string	(&(uid=%v)(objectclass=inetOrgPerson))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	inetOrgPerson:uid	An LDAP filter that maps the name of a user to an LDAP entry.

### ldapCache

Configure the attributes of the cache.

false

#### ldapCache > attributesCache

The attribute cache properties configuration.

false

Attribute name	Data type	Default value	Description
enabled	boolean	true	A Boolean value to indicate that the property is enabled.

Attribute name	Data type	Default value	Description
serverTTLAttribute	string		The time after which a cache entry expires. The subsequent call for this entry will be fetched directly from the server and then placed again in the cache.
size	int	2000	Defines the number of entities that can be stored in the cache. You can increase the size of the cache based on the number of entities that are required to be stored in the cache.
sizeLimit	int	2000	The size limit for the cache.
timeout	A period of time with millisecond precision	1200ms	Defines the maximum time that the contents of the LDAP attribute cache are available. When the specified time has elapsed, the LDAP attribute cache is cleared. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

#### ldapCache > searchResultsCache

The configuration for the search results cache.

false

Attribute name	Data type	Default value	Description
enabled	boolean	true	A Boolean value to indicate that the property is enabled.
resultsSizeLimit	int	2000	The maximum number of results that can be returned in the search.
size	int	2000	The size of the cache. The number of search results that are stored in the cache. This needs to be configured based on the number of search queries executed on the system and the hardware system resources available.

Attribute name	Data type	Default value	Description
timeout	A period of time with millisecond precision	1200ms	Defines the maximum time that the contents of the search results cache are available. When the specified time has elapsed, the search results cache is cleared. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

### **ldapEntityType**

Configure the LDAP object class, search filters, search bases and LDAP relative distinguished name (RDN) for Person, Group and Organizational Unit. For example, the Group entity type can have a search filter such as (&(ObjectCategory=Groupofnames)(ObjectClass=Groupofnames)) and the object class as Groupofnames with search base ou=iGroups,o=ibm,c=us.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		The name of the LDAP entity type.
searchFilter	string		A custom LDAP search expression used while searching for entity types. For example, searchFilter="(!(ObjectCategory=User)(ObjectClass=Groupofnames))"

#### **ldapEntityType > objectClass**

The object class defined for the given LDAP entity type in the LDAP server. For example, the object class for the group LDAP entity type can be Groupofnames.

false

string

#### **ldapEntityType > searchBase**

Specify the sub tree of the LDAP server for the search call for the given entity type which will override the base DN in search operations. For example, if the base DN is o=ibm,c=us and the search base for the PersonAccount entity type is defined to be ou=iUsers,o=ibm,c=us, then all search calls for PersonAccount will be made under subtree ou=iUsers,o=ibm,c=us. Multiple search bases can be configured for the same entity type.

false

string

### **netscapeFilters**

Specifies the list of default Netscape Directory Server LDAP filters.

false

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(!(objectclass=groupOfNames)(!(objectclass=groupOfUniqueNames)))	An LDAP filter clause for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	groupOfNames:member;groupOfUniqueMembers	An LDAP filter that identifies user to group memberships.
userFilter	string	(&(uid=%v)(objectclass=inetOrgPerson)	An LDAP filter clause for searching the user registry for users.
userIdMap	string	inetOrgPerson:uid	An LDAP filter that maps the name of a user to an LDAP entry.

### securewayFilters

Specifies the list of default IBM SecureWay Directory Server LDAP filters.

false

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(!(objectclass=groupOfNames)(!(objectclass=groupOfUniqueNames)))	An LDAP filter clause for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	groupOfNames:member;groupOfUniqueMembers	An LDAP filter that identifies user to group memberships.
userFilter	string	(&(uid=%v)(objectclass=ePerson))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	*:uid	An LDAP filter that maps the name of a user to an LDAP entry.

## Shared Library (library)

Shared Library

- file
- fileset
- folder

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
id	string		A unique configuration ID.
name	string		Name of shared library for administrators

### file

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

### fileset

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**WebSphere Optimized Local Adapters (WOLA) Connect (localAdaptersConnectService)**

Represents a z/OS Connect service implementation that uses WOLA to communicate with backend programs.

Attribute name	Data type	Default value	Description
connectionFactoryRef	A reference to top level connectionFactory element (string).		Reference to the configured connection factory element containing the JNDI name of the WOLA resource adapter connection factory to be used.
connectionWaitTimeout	int Minimum: 0 Maximum: 2147483647		Time to wait in seconds for an external address space application that matches the registration name to issue a WOLA Receive Request or Host Service API and become active.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
linkTaskChanCtxContEncoding	string	cp819	Defines the encoding of the data in all context containers that are sent to the destination program. This attribute is used when using the CICS Link Server and when the linkTaskChanID and useCICSContainer (true) attributes are also configured.
linkTaskChanCtxContHttpHeaders	string		Defines the HTTP header name or list of comma-separated and case-sensitive HTTP header names that are passed to the destination program using the context container with the name of ZCONHTTPHeaders. The information contained in this context container is in JSON format: {httpHeaders:{"header1":"header1Value", ..., "header-n":"headerValue-n"}}. If the request contains multiple headers with the same name, the value that is used is the one for the first header in the request. This attribute is used when using the CICS Link Server and when the linkTaskChanID and useCICSContainer (true) attributes are also configured.
linkTaskChanID	string		Defines the CICS channel name to use for delivering and receiving payloads using CICS containers. This attribute is used when using the CICS Link Server and when the useCICSContainer (true) attribute is also configured.
linkTaskChanReqContID	string	ZCONReqData	Defines the name of the request container. This attribute is used when using the CICS Link Server and when the linkTaskChanID and useCICSContainer (true) attributes are also configured.

Attribute name	Data type	Default value	Description
linkTaskChanRespContID	string	ZCONRespData	Defines the name of the response container. This attribute is used when using the CICS Link Server and when the linkTaskChanID and useCICSContainer (true) attributes are also configured.
linkTaskChanType	int Minimum: 0	0	Defines the type of CICS containers (0=CHAR, 1=BIT) that are to be associated with the configured channel ID. When set to 0=CHAR (default), the encoding of the character data in the input/output containers are expected/returned in ASCII (CCSID 819) and the data is converted to or from EBCDIC (cp037) before/after it is sent to/from the destination program. Use the BIT type to avoid data type and encoding expectations. This attribute is used when using the CICS Link Server and when the linkTaskChanID and useCICSContainer (true) attributes are also configured.
linkTaskReqContID	string		Defines the name of the request, or input, container. This attribute is used when using the CICS Link Server and when the linkTaskRspContID and useCICSContainer (true) attributes are also configured.
linkTaskReqContType	int Minimum: 0	0	Defines the type of the request container (0=CHAR, 1=BIT). This attribute is used when using the CICS Link Server and when the linkTaskReqContID and useCICSContainer (true) attributes are also configured.

Attribute name	Data type	Default value	Description
linkTaskRspContID	string		Defines the name of the response, or output, container. This attribute is used when using the CICS Link Server and when the linkTaskReqContID and useCICSContainer (true) attributes are also configured.
linkTaskRspContType	int Minimum: 0	0	Defines the type of the response container (0=CHAR, 1=BIT). This attribute is used when using the CICS Link Server and when the linkTaskRspContID and useCICSContainer (true) attributes are also configured.
linkTaskTranID	string		Defines the name of the WOLA CICS Link Server link invocation task transaction ID. This attribute is used when using the CICS Link Server.
registerName	string		WOLA target register name. This name must match the name an external address space application is using for the register name on a WOLA Register API call, or the name used for RGN with a WOLA CICS Link Server.
serviceName	string		WOLA target service name. This name must match the name an external address space application is using for the service name on a WOLA Receive Request or Host Service API call, or the program name used for SVC with a WOLA CICS Link Server.
useCICSContainer	boolean	false	Defines the mechanism to use for data propagation. When set to true, the payload is passed to the target CICS application program using CICS containers. When set to false (default), the payload is passed the target CICS application program using a COMMAREA. This attribute is used when using the CICS Link Server.

## Logging (logging)

Controls the capture and output of log and trace messages.

Attribute name	Data type	Default value	Description
consoleLogLevel	<ul style="list-style-type: none"><li>• ERROR</li><li>• WARNING</li><li>• AUDIT</li><li>• OFF</li><li>• INFO</li></ul>	AUDIT	<p>The logging level used to filter messages written to system streams. The default value is audit.</p> <p><b>ERROR</b> Error messages will be written to the system error stream.</p> <p><b>WARNING</b> Warning messages will be written to the system output stream. Error messages will be written to the system error stream.</p> <p><b>AUDIT</b> Audit and warning messages will be written to the system output stream. Error messages will be written to the system error stream.</p> <p><b>OFF</b> No server output will be written to system streams. Only JVM output will be written to system streams.</p> <p><b>INFO</b> Info, audit, and warning messages will be written to the system output stream. Error messages will be written to the system error stream.</p>

Attribute name	Data type	Default value	Description
copySystemStreams	boolean	true	If true, write System.out to the system output stream and System.err to the system error stream. If false, System.out and System.err will write to configured logs like messages.log or trace.log, but not to the system streams. The default value is true.
hideMessage	string		The list of messages, separated by a comma, that are configured to be hidden from the console.log and message.log files. If the messages are configured to be hidden, then they are redirected to the trace.log file.
logDirectory	Path to a directory	\${server.output.dir}/logs	Location of the directory for log files. The default value is \${server.output.dir}/logs.
maxFileSize	int Minimum: 0	20	Maximum size of a log file, in megabytes, before being rolled over; a value of 0 means no limit.
maxFiles	int Minimum: 0	2	Maximum number of log files that will be kept, before the oldest file is removed; a value of 0 means no limit.
messageFileName	string	messages.log	Name of the file to which message output will be written relative to the configured log directory. The default value is messages.log.
suppressSensitiveTrace	boolean	false	The server trace can expose sensitive data when tracing untyped data, such as bytes received over a network connection. If true, prevent potentially sensitive information from being exposed in log and trace files. The default value is false.
traceFileName	string	trace.log	Name of the file to which trace output will be written relative to the configured log directory. The default value is trace.log.

Attribute name	Data type	Default value	Description
traceFormat	<ul style="list-style-type: none"> <li>• ENHANCED</li> <li>• BASIC</li> <li>• ADVANCED</li> </ul>	ENHANCED	<p>This format is used for the trace log.</p> <p><b>ENHANCED</b> Use the enhanced basic trace format.</p> <p><b>BASIC</b> Use the basic trace format.</p> <p><b>ADVANCED</b> Use the advanced trace format.</p>
traceSpecification	string	*=info	<p>A trace specification that conforms to the trace specification grammar and specifies the initial state for various trace components. An empty value is allowed and treated as 'disable all trace'. Any component that is not specified is initialized to a default state of *=info.</p>

## Logstash Collector (logstashCollector)

Logstash collector gathers data from various sources and forwards the data to a logstash server using Lumberjack protocol.

- source

Attribute name	Data type	Default value	Description
hostName	string		Host name of the logstash server.
port	int Minimum: 1 Maximum: 65535		Port number of the logstash server.
sslRef	A reference to top level ssl element (string).		Specifies an ID of the SSL repertoire that is used to connect to the logstash server.

### source

Specifies a source to be used by the logstash collector.

false

string

## LTPA Token (ltpa)

Lightweight Third Party Authentication (LTPA) token configuration.

Attribute name	Data type	Default value	Description
expiration	A period of time with minute precision	120m	Amount of time after which a token expires in minutes. Specify a positive integer followed by a unit of time, which can be hours (h) or minutes (m). For example, specify 30 minutes as 30m. You can include multiple values in a single entry. For example, 1h30m is equivalent to 90 minutes.
keysFileName	Path to a file	\${server.output.dir}/resources/security/ltpa.keys	Path of the file containing the token keys.
keysPassword	Reversably encoded password (string)	{xor}CDo9Hgw=	Password for the token keys. The value can be stored in clear text or encoded form. It is recommended to encode the password, use the securityUtility tool with the encode option.
monitorInterval	A period of time with millisecond precision	0ms	Rate at which the server checks for updates to the LTPA token keys file. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

## Mail Session Object (mailSession)

Configuration for a Mail Session Instance.

- property

Attribute name	Data type	Default value	Description
description	string		Description of the Mail Session
from	string		The E-Mail address used to send mail with the Mail Session instance.
host	string		The host of the Mail Session
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
jndiName	string		Name of the Mail Session reference that is used for JNDI look-up
mailSessionID	string		The ID of the specific Mail Session Instance
password	Reversably encoded password (string)		The User's password, usually needed in order to connect to the host.
storeProtocol	string	imap	The Store Protocol used by the Mail Session instance. The default store protocol is IMAP
transportProtocol	string	smtp	The Transport Protocol used by the Mail Session instance. The default transport protocol is SMTP
user	string		The User's e-mail address used on the Host.

#### property

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		The name of the extra property
value	string		The value of the property that matches the name

## Managed Executor (managedExecutorService)

Managed executor service

- contextService
  - baseContext
    - baseContext
    - classloaderContext
    - jeeMetadataContext
    - securityContext
    - syncToOSThreadContext
    - zosWLMContext
  - classloaderContext
  - jeeMetadataContext
  - securityContext
  - syncToOSThreadContext
  - zosWLMContext

Attribute name	Data type	Default value	Description
contextServiceRef	A reference to top level contextService element (string).	DefaultContextService	Configures how context is propagated to threads
id	string		A unique configuration ID.
jndiName	string		JNDI name

### contextService

Configures how context is propagated to threads

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
jndiName	string		JNDI name
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

### contextService > baseContext

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
id	string		A unique configuration ID.
jndiName	string		JNDI name
onError	<ul style="list-style-type: none"><li>• IGNORE</li><li>• FAIL</li><li>• WARN</li></ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**contextService > baseContext > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

com.ibm.ws.context.service-factory

**contextService > baseContext > classloaderContext**

Classloader context propagation configuration.

false

**contextService > baseContext > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**contextService > baseContext > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**contextService > baseContext > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**contextService > baseContext > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"><li>• Propagate</li><li>• PropagateOrNew</li><li>• New</li></ul>	Propagate	Indicates how the WLM context should be handled for non-Daemon work. <b>Propagate</b> Use the same WLM Context (if one exists). <b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists. <b>New</b> Always create a new WLM context.

**contextService > classloaderContext**

Classloader context propagation configuration.

false

**contextService > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**contextService > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**contextService > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**contextService > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"> <li>• Propagate</li> <li>• PropagateOrNew</li> <li>• New</li> </ul>	Propagate	<p>Indicates how the WLM context should be handled for non-Daemon work.</p> <p><b>Propagate</b> Use the same WLM Context (if one exists).</p> <p><b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists.</p> <p><b>New</b> Always create a new WLM context.</p>

## Managed Scheduled Executor (managedScheduledExecutorService)

Managed scheduled executor service

- contextService
  - baseContext
    - baseContext
    - classloaderContext
    - jeeMetadataContext
    - securityContext
    - syncToOSThreadContext
    - zosWLMContext

- classloaderContext
- jeeMetadataContext
- securityContext
- syncToOSThreadContext
- zosWLMContext

Attribute name	Data type	Default value	Description
contextServiceRef	A reference to top level contextService element (string).	DefaultContextService	Configures how context is propagated to threads
id	string		A unique configuration ID.
jndiName	string		JNDI name

### contextService

Configures how context is propagated to threads

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**contextService > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
id	string		A unique configuration ID.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**contextService > baseContext > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

com.ibm.ws.context.service-factory

**contextService > baseContext > classloaderContext**

Classloader context propagation configuration.

false

**contextService > baseContext > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**contextService > baseContext > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**contextService > baseContext > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**contextService > baseContext > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"><li>• Propagate</li><li>• PropagateOrNew</li><li>• New</li></ul>	Propagate	Indicates how the WLM context should be handled for non-Daemon work.  <b>Propagate</b> Use the same WLM Context (if one exists).  <b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists.  <b>New</b> Always create a new WLM context.

**contextService > classloaderContext**

ClassLoader context propagation configuration.

false

**contextService > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**contextService > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**contextService > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**contextService > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"> <li>• Propagate</li> <li>• PropagateOrNew</li> <li>• New</li> </ul>	Propagate	<p>Indicates how the WLM context should be handled for non-Daemon work.</p> <p><b>Propagate</b> Use the same WLM Context (if one exists).</p> <p><b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists.</p> <p><b>New</b> Always create a new WLM context.</p>

## Managed Thread Factory (managedThreadFactory)

Managed thread factory

- contextService
  - baseContext
    - baseContext
    - classloaderContext
    - jeeMetadataContext
    - securityContext
    - syncToOSThreadContext
    - zosWLMContext
  - classloaderContext
  - jeeMetadataContext
  - securityContext
  - syncToOSThreadContext
  - zosWLMContext

Attribute name	Data type	Default value	Description
contextServiceRef	A reference to top level contextService element (string).	DefaultContextService	Configures how context is propagated to threads

Attribute name	Data type	Default value	Description
createDaemonThreads	boolean	false	Configures whether or not threads created by the managed thread factory should be daemon threads.
defaultPriority	int Minimum: 1 Maximum: 10		Default priority for threads created by the managed thread factory. If unspecified, the priority of the creating thread is used. Priority cannot exceed the maximum priority for the managed thread factory, in which case the maximum priority is used instead.
id	string		A unique configuration ID.
jndiName	string		JNDI name
maxPriority	int Minimum: 1 Maximum: 10		Maximum priority for threads created by the managed thread factory.

#### **contextService**

Configures how context is propagated to threads

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**contextService > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
id	string		A unique configuration ID.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**contextService > baseContext > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

com.ibm.ws.context.service-factory

**contextService > baseContext > classloaderContext**

Classloader context propagation configuration.

false

**contextService > baseContext > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**contextService > baseContext > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**contextService > baseContext > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**contextService > baseContext > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"><li>• Propagate</li><li>• PropagateOrNew</li><li>• New</li></ul>	Propagate	Indicates how the WLM context should be handled for non-Daemon work. <b>Propagate</b> Use the same WLM Context (if one exists). <b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists. <b>New</b> Always create a new WLM context.

**contextService > classloaderContext**

Classloader context propagation configuration.

false

**contextService > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**contextService > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**contextService > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**contextService > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"> <li>• Propagate</li> <li>• PropagateOrNew</li> <li>• New</li> </ul>	Propagate	<p>Indicates how the WLM context should be handled for non-Daemon work.</p> <p><b>Propagate</b> Use the same WLM Context (if one exists).</p> <p><b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists.</p> <p><b>New</b> Always create a new WLM context.</p>

## Messaging Engine (messagingEngine)

A messaging engine is a component, running inside a server, that manages messaging resources. Applications are connected to a messaging engine when they send and receive messages.

- alias
- fileStore
- messagingSecurity
  - role
    - group
    - queuePermission
      - action
    - tempDestinationPermission
      - action
    - topicPermission
      - action
    - user
- queue
- topicSpace

### alias

An alias destination maps an alternative name for a bus destination. You can use an alias destination for point-to-point messaging or publish/subscribe messaging.

false

Attribute name	Data type	Default value	Description
forceReliability	<ul style="list-style-type: none"> <li>AssuredPersistent</li> <li>BestEffortNonPersistent</li> <li>ReliableNonPersistent</li> <li>ExpressNonPersistent</li> <li>ReliablePersistent</li> </ul>	AssuredPersistent	<p>The reliability assigned to a message produced to this destination when an explicit reliability has not been set by the producer.</p> <p><b>AssuredPersistent</b> AssuredPersistent</p> <p><b>BestEffortNonPersistent</b> BestEffortNonPersistent</p> <p><b>ReliableNonPersistent</b> ReliableNonPersistent</p> <p><b>ExpressNonPersistent</b> ExpressNonPersistent</p> <p><b>ReliablePersistent</b> ReliablePersistent</p>
id	string		The name of the alias queue or alias topic space.
sendAllowed	<ul style="list-style-type: none"> <li>false</li> <li>true</li> </ul>	true	<p>Producers can send messages to this destination.</p> <p><b>false</b>    false</p> <p><b>true</b>     true</p>
targetDestination	string	Default.Queue	The target destination parameter identifies a destination that might be within the same Bus as the alias destination. By default, if no property is set, it points to Default.Queue.

### fileStore

Messaging file store.

false

Attribute name	Data type	Default value	Description
fileStoreSize	long Minimum: 20	400	The combined size in megabytes for both permanent and temporary store. The file store size is equally divided between permanent and temporary store. For example, if you specify 400 MB as file store size then 200 MB is used for permanent store and 200 MB is used for temporary store.

Attribute name	Data type	Default value	Description
logFileSize	long Minimum: 10	10	Size in megabytes of the log file. The log file size cannot exceed half the size of the file store size. For a file store size set to 400 MB, the log file size cannot exceed 200 MB. The maximum recommended log file size is 25% of the file store size. For a file store size set to 400 MB, the maximum recommended setting for log file size would be 100 MB.
path	string	\${server.output.dir}/messaging/messageStore	Path to the file store.

### **messagingSecurity**

Security for the wasJmsServer-1.0 feature.

false

#### **messagingSecurity > role**

A set of permissions that are mapped to the users and groups

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		The name of the role

#### **messagingSecurity > role > group**

Groups that are assigned to the role

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		The group that is defined as part of the user registry

#### **messagingSecurity > role > queuePermission**

Permission that is defined on a queue for a set of users and groups

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
queueRef	string		Reference to the Queue defined in the Messaging Engine

#### **messagingSecurity > role > queuePermission > action**

Operations that are allowed on the destination

false

**messagingSecurity > role > tempDestinationPermission**

Permission that is defined on a temporary destination for a set of users and groups

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
prefix	string		Prefix defined for a temporary destination

**messagingSecurity > role > tempDestinationPermission > action**

Operations that are allowed on the destination

false

**messagingSecurity > role > topicPermission**

Permission that is defined on a topic for a set of users and groups

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
topicName	string		Name of the Topic inside the TopicSpace
topicSpaceRef	string	Default.Topic.Space	Reference to the TopicSpace defined in the Messaging Engine

**messagingSecurity > role > topicPermission > action**

Operations that are allowed on the destination

false

**messagingSecurity > role > user**

Users that are assigned to the particular role

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		The user that is defined as part of the registry

**queue**

A queue destination represents a message queue and is used for point-to-point messaging.

false

Attribute name	Data type	Default value	Description
exceptionDestination	string	_SYSTEM.Exception.Destination	The destination to which a message is forwarded by the system when it cannot be delivered to this destination.

Attribute name	Data type	Default value	Description
failedDeliveryPolicy	<ul style="list-style-type: none"> <li>KEEP_TRYING</li> <li>SEND_TO_EXCEPTION_DESTINATION</li> <li>DISCARD</li> </ul>	SEND_TO_EXCEPTION_DESTINATION	<p>Indicates that the messaging engine must take when the maxredeliverycount is reached for a message.</p> <p><b>KEEP_TRYING</b> KEEP_TRYING</p> <p><b>SEND_TO_EXCEPTION_DESTINATION</b> SEND_TO_EXCEPTION_DESTINATION</p> <p><b>DISCARD</b> DISCARD</p>
forceReliability	<ul style="list-style-type: none"> <li>AssuredPersistent</li> <li>BestEffortNonPersistent</li> <li>ReliableNonPersistent</li> <li>ExpressNonPersistent</li> <li>ReliablePersistent</li> </ul>	AssuredPersistent	<p>The reliability assigned to a message produced to this destination when an explicit reliability has not been set by the producer.</p> <p><b>AssuredPersistent</b> AssuredPersistent</p> <p><b>BestEffortNonPersistent</b> BestEffortNonPersistent</p> <p><b>ReliableNonPersistent</b> ReliableNonPersistent</p> <p><b>ExpressNonPersistent</b> ExpressNonPersistent</p> <p><b>ReliablePersistent</b> ReliablePersistent</p>
id	string		The name of the queue.
maintainStrictOrder	boolean	false	Maintains the order in which a producer sends messages to the destination.
maxMessageDepth	long Minimum: 1	50000	The maximum number of messages that the messaging engine can place on its message points.
maxRedeliveryCount	int	5	The maximum number of failed attempts to process a message. After this number of failed attempts, if an exception destination is configured, the message is forwarded from the intended destination to its exception destination. If an exception destination is not configured, a time interval between retry attempts is applied.
receiveAllowed	boolean	true	Clear this option (setting it to false) to prevent consumers from being able to receive messages from this destination.

Attribute name	Data type	Default value	Description
redeliveryInterval	long	5000	When no exception destination is configured, the time interval to apply between retry attempts, after the maximum failed deliveries limit is reached, for this destination.
sendAllowed	boolean	true	Producers can send messages to this destination.

### topicSpace

A topic space destination represents a set of "publish and subscribe" topics and is used for publish/subscribe messaging.

false

Attribute name	Data type	Default value	Description
exceptionDestination	string	_SYSTEM.Exception.Destination	The destination to which a message is forwarded by the system when it cannot be delivered to this destination.
failedDeliveryPolicy	<ul style="list-style-type: none"> <li>KEEP_TRYING</li> <li>SEND_TO_EXCEPTION_DESTINATION</li> <li>DISCARD</li> </ul>	SEND_TO_EXCEPTION_DESTINATION	<p>Actions that the messaging engine must take when the maxredeliverycount is reached for a message.</p> <p><b>KEEP_TRYING</b> KEEP_TRYING</p> <p><b>SEND_TO_EXCEPTION_DESTINATION</b> SEND_TO_EXCEPTION_DESTINATION</p> <p><b>DISCARD</b> DISCARD</p>
forceReliability	<ul style="list-style-type: none"> <li>AssuredPersistent</li> <li>BestEffortNonPersistent</li> <li>ReliableNonPersistent</li> <li>ExpressNonPersistent</li> <li>ReliablePersistent</li> </ul>	AssuredPersistent	<p>The reliability assigned to a message produced to this destination when an explicit reliability has not been set by the producer.</p> <p><b>AssuredPersistent</b> AssuredPersistent</p> <p><b>BestEffortNonPersistent</b> BestEffortNonPersistent</p> <p><b>ReliableNonPersistent</b> ReliableNonPersistent</p> <p><b>ExpressNonPersistent</b> ExpressNonPersistent</p> <p><b>ReliablePersistent</b> ReliablePersistent</p>
id	string		The name of the topic space.

Attribute name	Data type	Default value	Description
maintainStrictOrder	boolean	false	Maintains the order in which a producer sends messages to the destination.
maxMessageDepth	long Minimum: 1	50000	The maximum number of messages that the messaging engine can place on its message points.
maxRedeliveryCount	int	5	The maximum number of failed attempts to process a message. After this number of failed attempts, if an exception destination is configured, the message is forwarded from the intended destination to its exception destination. If an exception destination is not configured, a time interval between retry attempts is applied.
receiveAllowed	boolean	true	Clear this option (setting it to false) to prevent consumers from being able to receive messages from this destination.
redeliveryInterval	long	5000	When no exception destination is configured, the time interval to apply between retry attempts, after the maximum failed deliveries limit is reached, for this destination.
sendAllowed	boolean	true	Producers can send messages to this destination.

## Default Mime Types (mimeTypes)

Definition of mime types shared by all http virtual hosts

- type

### type

Definition of mime type as id=value. Use the extension as the id, and the associated type as the value.

false

string

## Mongo (mongo)

Configuration for a Mongo instance.

- hostNames
- library
  - file

- fileset
- folder
- ports

Attribute name	Data type	Default value	Description
autoConnectRetry	boolean		Retry connections to a server, for an interval up to the <code>maxAutoConnectRetryTime</code> , if the socket cannot be opened.
connectTimeout	A period of time with millisecond precision		Connection timeout for new connections. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
connectionsPerHost	int Minimum: 0		Limits the number of open connections to each host. Connections are pooled when not in use.
cursorFinalizerEnabled	boolean		Attempts to clean up <code>DBCursors</code> that are not closed.
description	string		Description of a Mongo instance.
id	string		A unique configuration ID.
libraryRef	A reference to top level library element (string).		Specifies a library that contains the MongoDB Java Driver.
maxAutoConnectRetryTime	A period of time with millisecond precision		Interval during which to retry attempts to open a connection to a server. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
maxWaitTime	A period of time with millisecond precision		Maximum amount of time to wait for an available connection. If negative, the connection request never times out. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>
password	Reversably encoded password (string)		Password for database user.
readPreference	<ul style="list-style-type: none"> <li>• primary</li> <li>• secondaryPreferred</li> <li>• secondary</li> <li>• primaryPreferred</li> <li>• nearest</li> </ul>		<p>Configures the read preference.</p> <p><b>primary</b> primary</p> <p><b>secondaryPreferred</b> secondaryPreferred</p> <p><b>secondary</b> secondary</p> <p><b>primaryPreferred</b> primaryPreferred</p> <p><b>nearest</b> nearest</p>
socketKeepAlive	boolean		Configures whether or not to keep sockets alive.

Attribute name	Data type	Default value	Description
socketTimeout	A period of time with millisecond precision		The socket timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
threadsAllowedToBlockForConnectionMultiplier	Minimum: 0		This value, multiplied by connectionsPerHost, establishes an upper limit on threads that are allowed to wait for an available connection.
user	string		Database user name.
writeConcern	<ul style="list-style-type: none"> <li>• ERRORS_IGNORED</li> <li>• ACKNOWLEDGED</li> <li>• SAFE</li> <li>• JOURNALED</li> <li>• NORMAL</li> <li>• REPLICAS_SAFE</li> <li>• FSYNC_SAFE</li> <li>• MAJORITY</li> <li>• FSYNCED</li> <li>• JOURNAL_SAFE</li> <li>• REPLICAS_SAFE</li> <li>• NONE</li> <li>• UNACKNOWLEDGED</li> </ul>		<p>The reliability of a write operation to the mongo server.</p> <p><b>ERRORS_IGNORED</b> ERRORS_IGNORED</p> <p><b>ACKNOWLEDGED</b> ACKNOWLEDGED</p> <p><b>SAFE</b> SAFE</p> <p><b>JOURNALED</b> JOURNALED</p> <p><b>NORMAL</b> NORMAL</p> <p><b>REPLICAS_SAFE</b> REPLICAS_SAFE</p> <p><b>FSYNC_SAFE</b> FSYNC_SAFE</p> <p><b>MAJORITY</b> MAJORITY</p> <p><b>FSYNCED</b> FSYNCED</p> <p><b>JOURNAL_SAFE</b> JOURNAL_SAFE</p> <p><b>REPLICAS_SAFE</b> REPLICAS_SAFE</p> <p><b>NONE</b> NONE</p> <p><b>UNACKNOWLEDGED</b> UNACKNOWLEDGED</p>

**hostNames**

List of host names. The ordering of this list must be consistent with the list of ports, such that the first element in the list of host names corresponds to the first element in the list of ports, and so forth.

false

string

**library**

Specifies a library that contains the MongoDB Java Driver.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

**library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

#### library > folder

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

#### ports

List of port numbers. The ordering of this list must be consistent with the list of host names, such that the first element in the list of host names corresponds to the first element in the list of ports, and so forth.

false

## MongoDB DB (mongoDB)

Configuration for a MongoDB DB instance.

- mongo
  - hostNames
  - library
    - file
    - fileset
    - folder
  - ports

Attribute name	Data type	Default value	Description
databaseName	string		Name of the database.
id	string		A unique configuration ID.
jndiName	string		JNDI name for a MongoDB DB instance
mongoRef	A reference to top level mongo element (string).		Specifies the Mongo instance that this DB instance belongs to.

### mongo

Specifies the Mongo instance that this DB instance belongs to.

false

Attribute name	Data type	Default value	Description
autoConnectRetry	boolean		Retry connections to a server, for an interval up to the maxAutoConnectRetryTime, if the socket cannot be opened.
connectTimeout	A period of time with millisecond precision		Connection timeout for new connections. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
connectionsPerHost	int Minimum: 0		Limits the number of open connections to each host. Connections are pooled when not in use.
cursorFinalizerEnabled	boolean		Attempts to clean up DBCursors that are not closed.
description	string		Description of a Mongo instance.
libraryRef	A reference to top level library element (string).		Specifies a library that contains the MongoDB Java Driver.

Attribute name	Data type	Default value	Description
maxAutoConnectRetryTime	A period of time with millisecond precision		Interval during which to retry attempts to open a connection to a server. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
maxWaitTime	A period of time with millisecond precision		Maximum amount of time to wait for an available connection. If negative, the connection request never times out. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>
password	Reversably encoded password (string)		Password for database user.

Attribute name	Data type	Default value	Description
readPreference	<ul style="list-style-type: none"> <li>• primary</li> <li>• secondaryPreferred</li> <li>• secondary</li> <li>• primaryPreferred</li> <li>• nearest</li> </ul>		<p>Configures the read preference.</p> <p><b>primary</b> primary</p> <p><b>secondaryPreferred</b> secondaryPreferred</p> <p><b>secondary</b> secondary</p> <p><b>primaryPreferred</b> primaryPreferred</p> <p><b>nearest</b> nearest</p>
socketKeepAlive	boolean		Configures whether or not to keep sockets alive.
socketTimeout	A period of time with millisecond precision		The socket timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
threadsAllowedToBlockForConnectionMultiplier	<p>Minimum: 0</p>		This value, multiplied by connectionsPerHost, establishes an upper limit on threads that are allowed to wait for an available connection.
user	string		Database user name.

Attribute name	Data type	Default value	Description
writeConcern	<ul style="list-style-type: none"> <li>• ERRORS_IGNORED</li> <li>• ACKNOWLEDGED</li> <li>• SAFE</li> <li>• JOURNALED</li> <li>• NORMAL</li> <li>•</li> <li>• REPLICAS_SAFE</li> <li>• FSYNC_SAFE</li> <li>• MAJORITY</li> <li>• FSYNCED</li> <li>• JOURNAL_SAFE</li> <li>• REPLICAS_SAFE</li> <li>• NONE</li> <li>• UNACKNOWLEDGED</li> </ul>		<p>The reliability of a write operation to the mongo server.</p> <p><b>ERRORS_IGNORED</b> ERRORS_IGNORED</p> <p><b>ACKNOWLEDGED</b> ACKNOWLEDGED</p> <p><b>SAFE</b> SAFE</p> <p><b>JOURNALED</b> JOURNALED</p> <p><b>NORMAL</b> NORMAL</p> <p><b>REPLICAS_SAFE</b> REPLICAS_SAFE</p> <p><b>FSYNC_SAFE</b> FSYNC_SAFE</p> <p><b>MAJORITY</b> MAJORITY</p> <p><b>FSYNCED</b> FSYNCED</p> <p><b>JOURNAL_SAFE</b> JOURNAL_SAFE</p> <p><b>REPLICAS_SAFE</b> REPLICAS_SAFE</p> <p><b>NONE</b> NONE</p> <p><b>UNACKNOWLEDGED</b> UNACKNOWLEDGED</p>

**mongo > hostNames**

List of host names. The ordering of this list must be consistent with the list of ports, such that the first element in the list of host names corresponds to the first element in the list of ports, and so forth.

false

string

**mongo > library**

Specifies a library that contains the MongoDB Java Driver.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.

Attribute name	Data type	Default value	Description
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

**mongo > library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**mongo > library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**mongo > library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**mongo > ports**

List of port numbers. The ordering of this list must be consistent with the list of host names, such that the first element in the list of host names corresponds to the first element in the list of ports, and so forth.

false

## Monitor (monitor)

Configuration for Monitoring Feature which includes enabled traditional PMI ,FineGrained and any future configurations updates.

Attribute name	Data type	Default value	Description
enableTraditionalPMI	boolean	false	Property to enable or disable Traditional PMI way of reporting.
filter	string		Allows user to enable/disable monitors based on group name such as WebContainer,JVM,ThreadPool,Session,Conn and so on.

## RRS Native Transaction Manager (nativeTransactionManager)

Configures the RRS Native Transaction Manager.

Attribute name	Data type	Default value	Description
resourceManagerNamePrefix	string	DEFAULT	The resource manager prefix to be used as part of the server generated resource manager name that is registered with Resource Recovery Services (RRS). The prefix must contain 1 to 8 alphanumeric (A-Z,a-z,0-9) and national (@,#,\$) character only. The prefix name of DEFAULT is a reserved prefix name that identifies a default server configuration and should not be used for securing server access.
shutdownTimeout	A period of time with millisecond precision	15s	The amount of time to wait before allowing the native context manager to stop if one or more native contexts are in-use. A native context is considered in-use if it contains an RRS unit of recovery with one or more interests. The timeout is specified by a positive integer followed by a unit of time, which can be milliseconds (ms), seconds (s), minutes (m) or hours (h). For example, fifteen seconds is specified as 15s. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

## Netscape Directory Server LDAP Filters (netscapeLdapFilterProperties)

Specifies the list of default Netscape Directory Server LDAP filters.

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(1(objectclass=groupOfNames)(1(objectclass=groupOfUniqueNames))))	An LDAP filter clause for groups.

Attribute name	Data type	Default value	Description
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	groupOfNames:member;groupOfUniqueMembers	An LDAP filter that identifies user to group memberships.
id	string		A unique configuration ID.
userFilter	string	(&(uid=%v)(objectclass=inetOrgPerson))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	inetOrgPerson:uid	An LDAP filter that maps the name of a user to an LDAP entry.

## OAuth Role Map (oauth-roles)

OAuth web application security role map.

- authenticated
  - group
  - special-subject
  - user
- clientManager
  - group
  - special-subject
  - user

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

### authenticated

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

### authenticated > group

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		A group access ID in the general form group:realmName/groupUniqueId. A value will be generated if one is not specified.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
name	string		Name of a group that has the security role.

**authenticated > special-subject**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
type	<ul style="list-style-type: none"> <li>• EVERYONE</li> <li>• ALL_AUTHENTICATED_USERS</li> </ul>		<p>One of the following special subject types: ALL_AUTHENTICATED_USERS, EVERYONE.</p> <p><b>EVERYONE</b> All users for every request, even if the request was not authenticated.</p> <p><b>ALL_AUTHENTICATED_USERS</b> All authenticated users.</p>

**authenticated > user**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		A user access ID in the general form user:realmName/userUniqueId. A value will be generated if one is not specified.
id	string		A unique configuration ID.
name	string		Name of a user who has the security role.

**clientManager**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

**clientManager > group**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		A group access ID in the general form group:realmName/groupUniqueId. A value will be generated if one is not specified.
id	string		A unique configuration ID.
name	string		Name of a group that has the security role.

#### clientManager > special-subject

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
type	<ul style="list-style-type: none"> <li>• EVERYONE</li> <li>• ALL_AUTHENTICATED_USERS</li> </ul>		<p>One of the following special subject types: ALL_AUTHENTICATED_USERS, EVERYONE.</p> <p><b>EVERYONE</b> All users for every request, even if the request was not authenticated.</p> <p><b>ALL_AUTHENTICATED_USERS</b> All authenticated users.</p>

#### clientManager > user

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		A user access ID in the general form user:realmName/userUniqueId. A value will be generated if one is not specified.
id	string		A unique configuration ID.
name	string		Name of a user who has the security role.

## OAuth Provider Definition (oauthProvider)

OAuth provider definition.

- autoAuthorizeClient
- databaseStore
  - dataSource

- connectionManager
- containerAuthData
- jaasLoginContextEntry
- jdbcDriver
  - library
    - file
    - fileset
    - folder
- properties
- properties.datadirect.sqlserver
- properties.db2.i.native
- properties.db2.i.toolbox
- properties.db2.jcc
- properties.derby.client
- properties.derby.embedded
- properties.informix
- properties.informix.jcc
- properties.microsoft.sqlserver
- properties.oracle
- properties.sybase
- recoveryAuthData
- grantType
- jwtGrantType
- library
  - file
  - fileset
  - folder
- localStore
  - client
    - functionalUserGroupIds
    - grantTypes
    - postLogoutRedirectUris
    - redirect
    - responseTypes
- mediatorClassname

Attribute name	Data type	Default value	Description
accessTokenLength	long	40	Length of the generated OAuth access token. The equivalent provider parameter in the full application server profile is <code>oauth20.access.token.length</code> .

Attribute name	Data type	Default value	Description
accessTokenLifetime	A period of time with second precision	7200	Time that access token is valid (seconds). The equivalent provider parameter in the full application server profile is <code>oauth20.token.lifetime.seconds</code> . Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
allowPublicClients	boolean	false	A value of false disables the access of public clients as detailed in the OAuth specification. The equivalent provider parameter in the full application server profile is <code>oauth20.allow.public.clients</code> .
authorizationCodeLength	long	30	Length of the generated authorization code. The equivalent provider parameter in the full application server profile is <code>oauth20.code.length</code> .
authorizationCodeLifetime	A period of time with second precision	60	Authorization code lifetime (seconds). The equivalent provider parameter in the full application server profile is <code>oauth20.code.lifetime.seconds</code> . Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
authorizationErrorTemplate	string		URL of a custom authorization error page template. The equivalent provider parameter in the full application server profile is <code>oauth20.authorization.error.template</code> .

Attribute name	Data type	Default value	Description
authorizationFormTemplate	string	template.html	URL of a custom authorization page template. The equivalent provider parameter in the full application server profile is <code>oauth20.authorization.form.template</code> .
authorizationGrantLifetime	A period of time with second precision	604800	Authorization grant lifetime (seconds). The equivalent provider parameter in the full application server profile is <code>oauth20.max.authorization.grant.lifetime.seconds</code> . Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
autoAuthorize	boolean	false	To use auto authorization, append the <code>autoAuthorize</code> parameter to requests with a value of true. The equivalent provider parameter in the full application server profile is <code>oauth20.autoauthorize.param</code> .
autoAuthorizeParam	string	autoauthz	To use auto authorization, append the <code>autoAuthorize</code> parameter to requests with a value of true. The equivalent provider parameter in the full application server profile is <code>oauth20.autoauthorize.param</code> .
certAuthentication	boolean	false	Enable the authentication of client certificate in the https request.
characterEncoding	string		Set request character encoding to this value. The equivalent provider parameter in the full application server profile is <code>characterEncoding</code> .
clientTokenCacheSize	long		Maximum number of entries in the client token cache.

Attribute name	Data type	Default value	Description
clientURISubstitutions	string		Optional value to replace client URI strings for dynamic hostnames. The equivalent provider parameter in the full application server profile is <code>oauth20.client.uri.substitutions</code> .
consentCacheEntryLifetime	A period of time with second precision	1800	Time that an entry in the consent cache is valid (seconds). Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
consentCacheSize	long Minimum: 0	1000	Maximum number of entries allowed in the consent cache.
coverageMapSessionMaxAge	A period of time with second precision	600	The max-age value (seconds) for the cache-control header of the coverage map service. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
customLoginURL	string	login.jsp	URL of a custom login page. The equivalent provider parameter in the full application server profile is <code>oauth20.authorization.loginURL</code> .
filter	string		URI filter selects requests to be authorized by this provider. The equivalent provider parameter in the full application server profile is <code>Filter</code> .
httpsRequired	boolean	true	SSL communication between the OAuth client and provider is required.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
includeTokenInSubject	boolean	true	If the value is true, add the com.ibm.wsspi.security.oauth2.token.WSOAuth2Token as a private credential. The equivalent provider parameter in the full application server profile is includeToken.
issueRefreshToken	boolean	true	A value of false disables generation and the use of refresh tokens. The equivalent provider parameter in the full application server profile is oauth20.issue.refresh.token.
libraryRef	A reference to top level library element (string).		Reference to shared library containing the mediator plugin class.
oauthOnly	boolean	true	If the value is true, then requests matching the filter must have an access token or they will be failed. If false, then matching requests will be checked for other authentication data if no access token is present. The equivalent provider parameter in the full application server profile is oauthOnly.
refreshTokenLength	long	50	Length of generated refresh token. The equivalent provider parameter in the full application server profile is oauth20.refresh.token.length.
skipResourceOwnerValidation	boolean	false	If the value is true, skip validation of resource owner.
userClientTokenLimit	long		Token limit for each user and client combination.

#### **autoAuthorizeClient**

Name of a client that is allowed to use auto authorization. The equivalent provider parameter in the full application server profile is oauth20.autoauthorize.clients.

false

string

#### **databaseStore**

Clients are defined and tokens are cached in the database.

false

Attribute name	Data type	Default value	Description
cleanupExpiredTokenInterval	A period of time with second precision	3600	Expired token cleanup interval (seconds). The equivalent provider parameter in the full application server profile is <code>oauthjdbc.CleanupInterval</code> . Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
dataSourceRef	A reference to top level <code>dataSource</code> element (string).		Reference to the data source for the store.
password	Reversably encoded password (string)		Password used to access the database.
schema	string	OAuthDBSchema	Schema
user	string		User

#### databaseStore > dataSource

Reference to the data source for the store.

false

Attribute name	Data type	Default value	Description
beginTranForResultSetScrolling	boolean	true	Attempt transaction enlistment when result set scrolling interfaces are used.
beginTranForVendorAPIs	boolean	true	Attempt transaction enlistment when vendor interfaces are used.
commitOrRollbackOnCleanup	<ul style="list-style-type: none"> <li>• commit</li> <li>• rollback</li> </ul>		<p>Determines how to clean up connections that might be in a database unit of work (<code>AutoCommit=false</code>) when the connection is closed or returned to the pool.</p> <p><b>commit</b> Clean up the connection by committing.</p> <p><b>rollback</b> Clean up the connection by rolling back.</p>
connectionManagerRef	A reference to top level <code>connectionManager</code> element (string).		Connection manager for a data source.

Attribute name	Data type	Default value	Description
connectionSharing	<ul style="list-style-type: none"> <li>MatchOriginalRequest</li> <li>MatchCurrentState</li> </ul>	MatchOriginalRequest	<p>Specifies how connections are matched for sharing.</p> <p><b>MatchOriginalRequest</b> When sharing connections, match based on the original connection request.</p> <p><b>MatchCurrentState</b> When sharing connections, match based on the current state of the connection.</p>
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.
enableConnectionCasting	boolean	false	Indicates that connections obtained from the data source should be castable to interface classes that the JDBC vendor connection implementation implements. Enabling this option incurs additional overhead on each getConnection operation. If vendor JDBC interfaces are needed less frequently, it might be more efficient to leave this option disabled and use Connection.unwrap(interface) only where it is needed.

Attribute name	Data type	Default value	Description
isolationLevel	<ul style="list-style-type: none"> <li>• TRANSACTION_REPEATABLE_READ</li> <li>• TRANSACTION_READ_COMMITTED</li> <li>• TRANSACTION_SERIALIZABLE</li> <li>• TRANSACTION_READ_UNCOMMITTED</li> <li>• TRANSACTION_SNAPSHOT</li> </ul>		<p>Default transaction isolation level.</p> <p><b>TRANSACTION_REPEATABLE_READ</b> Dirty reads and non-repeatable reads are prevented; phantom reads can occur.</p> <p><b>TRANSACTION_READ_COMMITTED</b> Dirty reads are prevented; non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SERIALIZABLE</b> Dirty reads, non-repeatable reads and phantom reads are prevented.</p> <p><b>TRANSACTION_READ_UNCOMMITTED</b> Dirty reads, non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SNAPSHOT</b> Snapshot isolation for Microsoft SQL Server JDBC Driver and DataDirect Connect for JDBC driver.</p>
jaasLoginContextEntryRef	A reference to top level jaasLoginContextEntry element (string).		JAAS login context entry for authentication.
jdbcDriverRef	A reference to top level jdbcDriver element (string).		JDBC driver for a data source.
jndiName	string		JNDI name for a data source.

Attribute name	Data type	Default value	Description
queryTimeout	A period of time with second precision		Default query timeout for SQL statements. In a JTA transaction, syncQueryTimeoutWithTransactionTimeout can override this default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.
statementCacheSize	int Minimum: 0	10	Maximum number of cached statements per connection.
supplementalJDBCTrace	boolean		Supplements the JDBC driver trace that is logged when JDBC driver trace is enabled in bootstrap.properties. JDBC driver trace specifications include: com.ibm.ws.database.logwriter, com.ibm.ws.db2.logwriter, com.ibm.ws.derby.logwriter, com.ibm.ws.informix.logwriter, com.ibm.ws.oracle.logwriter, com.ibm.ws.sqlserver.logwriter, com.ibm.ws.sybase.logwriter
syncQueryTimeoutWithTransactionTimeout	boolean	false	Use the time remaining (if any) in a JTA transaction as the default query timeout for SQL statements.
transactional	boolean	true	Enable participation in transactions that are managed by the application server.
type	<ul style="list-style-type: none"> <li>javax.sql.DataSource</li> <li>javax.sql.XADataSource</li> <li>javax.sql.ConnectionPoolDataSource</li> </ul>		Type of data source. <b>javax.sql.DataSource</b> javax.sql.DataSource <b>javax.sql.XADataSource</b> javax.sql.XADataSource <b>javax.sql.ConnectionPoolDataSource</b> javax.sql.ConnectionPoolDataSource

**databaseStore > dataSource > connectionManager**

Connection manager for a data source.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.

Attribute name	Data type	Default value	Description
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**databaseStore > dataSource > containerAuthData**

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

**databaseStore > dataSource > jaasLoginContextEntry**

JAAS login context entry for authentication.

false

Attribute name	Data type	Default value	Description
loginModuleRef	List of references to top level jaasLoginModule elements (comma-separated string).	hashtable,userNameAndPassword,certificate,clientId	Word, certificate, clientId of a JAAS login module.
name	string		Name of a JAAS configuration entry.

**databaseStore > dataSource > jdbcDriver**

JDBC driver for a data source.

false

Attribute name	Data type	Default value	Description
javax.sql.ConnectionPoolDataSource	string		JDBC driver implementation of javax.sql.ConnectionPoolDataSource.
javax.sql.DataSource	string		JDBC driver implementation of javax.sql.DataSource.
javax.sql.XADataSource	string		JDBC driver implementation of javax.sql.XADataSource.
libraryRef	A reference to top level library element (string).		Identifies JDBC driver JARs and native files.

**databaseStore > dataSource > jdbcDriver > library**

Identifies JDBC driver JARs and native files.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

**databaseStore > dataSource > jdbcDriver > library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**databaseStore > dataSource > jdbcDriver > library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**databaseStore > dataSource > jdbcDriver > library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**databaseStore > dataSource > properties**

List of JDBC vendor properties for the data source. For example, databaseName="dbname" serverName="localhost" portNumber="50000".

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database.
databaseName	string		JDBC driver property: databaseName.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
serverName	string		Server where the database is running.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**databaseStore > dataSource > properties.datadirect.sqlserver**

Data source properties for the DataDirect Connect for JDBC driver for Microsoft SQL Server.

false

Attribute name	Data type	Default value	Description
JDBCBehavior	<ul style="list-style-type: none"> <li>• 1</li> <li>• 0</li> </ul>	0	JDBC driver property: JDBCBehavior. Values are: 0 (JDBC 4.0) or 1 (JDBC 3.0). <b>1</b> JDBC 3.0 <b>0</b> JDBC 4.0
XATransactionGroup	string		JDBC driver property: XATransactionGroup.
XMLDescribeType	<ul style="list-style-type: none"> <li>• longvarbinary</li> <li>• longvarchar</li> </ul>		JDBC driver property: XMLDescribeType. <b>longvarbinary</b> longvarbinary <b>longvarchar</b> longvarchar
accountingInfo	string		JDBC driver property: accountingInfo.
alternateServers	string		JDBC driver property: alternateServers.
alwaysReportTriggerResults	boolean		JDBC driver property: alwaysReportTriggerResults.
applicationName	string		JDBC driver property: applicationName.
authenticationMethod	<ul style="list-style-type: none"> <li>• ntlm</li> <li>• userIdPassword</li> <li>• kerberos</li> <li>• auto</li> </ul>		JDBC driver property: authenticationMethod. <b>ntlm</b> ntlm <b>userIdPassword</b> userIdPassword <b>kerberos</b> kerberos <b>auto</b> auto
bulkLoadBatchSize	long		JDBC driver property: bulkLoadBatchSize.
bulkLoadOptions	long		JDBC driver property: bulkLoadOptions.
clientHostName	string		JDBC driver property: clientHostName.
clientUser	string		JDBC driver property: clientUser.

Attribute name	Data type	Default value	Description
codePageOverride	string		JDBC driver property: codePageOverride.
connectionRetryCount	int		JDBC driver property: connectionRetryCount.
connectionRetryDelay	A period of time with second precision		JDBC driver property: connectionRetryDelay. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
convertNull	int		JDBC driver property: convertNull.
databaseName	string		JDBC driver property: databaseName.
dateTimeInputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeInputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
dateTimeOutputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeOutputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
describeInputParameters	<ul style="list-style-type: none"> <li>• describeIfString</li> <li>• noDescribe</li> <li>• describeIfDateTime</li> <li>• describeAll</li> </ul>		JDBC driver property: describeInputParameters.  <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll

Attribute name	Data type	Default value	Description
describeOutputParameters	<ul style="list-style-type: none"> <li>describeIfString</li> <li>noDescribe</li> <li>describeIfDateTime</li> <li>describeAll</li> </ul>		JDBC driver property: describeOutputParameters. <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll
enableBulkLoad	boolean		JDBC driver property: enableBulkLoad.
enableCancelTimeout	boolean		JDBC driver property: enableCancelTimeout.
encryptionMethod	<ul style="list-style-type: none"> <li>loginSSL</li> <li>requestSSL</li> <li>SSL</li> <li>noEncryption</li> </ul>		JDBC driver property: encryptionMethod. <b>loginSSL</b> loginSSL <b>requestSSL</b> requestSSL <b>SSL</b> SSL <b>noEncryption</b> noEncryption
failoverGranularity	<ul style="list-style-type: none"> <li>disableIntegrityCheck</li> <li>atomicWithRepositioning</li> <li>nonAtomic</li> <li>atomic</li> </ul>		JDBC driver property: failoverGranularity. <b>disableIntegrityCheck</b> disableIntegrityCheck <b>atomicWithRepositioning</b> atomicWithRepositioning <b>nonAtomic</b> nonAtomic <b>atomic</b> atomic
failoverMode	<ul style="list-style-type: none"> <li>connect</li> <li>select</li> <li>extended</li> </ul>		JDBC driver property: failoverMode. <b>connect</b> connect <b>select</b> select <b>extended</b> extended
failoverPreconnect	boolean		JDBC driver property: failoverPreconnect.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
initializationString	string		JDBC driver property: initializationString.
insensitiveResultSetBufferSize	int		JDBC driver property: insensitiveResultSetBufferSize.

Attribute name	Data type	Default value	Description
javaDoubleToString	boolean		JDBC driver property: javaDoubleToString.
loadBalancing	boolean		JDBC driver property: loadBalancing.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
longDataCacheSize	int Minimum: -1		JDBC driver property: longDataCacheSize.
netAddress	string		JDBC driver property: netAddress.
packetSize	int Minimum: -1 Maximum: 128		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
queryTimeout	A period of time with second precision		JDBC driver property: queryTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
resultsetMetaDataOptions	int		JDBC driver property: resultSetMetaDataOptions.
selectMethod	<ul style="list-style-type: none"> <li>• direct</li> <li>• cursor</li> </ul>		JDBC driver property: selectMethod.  <b>direct</b> direct <b>cursor</b> cursor
serverName	string	localhost	Server where the database is running.
snapshotSerializable	boolean		JDBC driver property: snapshotSerializable.

Attribute name	Data type	Default value	Description
spyAttributes	string		JDBC driver property: spyAttributes.
stringInputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringInputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
stringOutputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringOutputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
suppressConnectionWarnings	boolean		JDBC driver property: suppressConnectionWarnings.
transactionMode	<ul style="list-style-type: none"> <li>explicit</li> <li>implicit</li> </ul>		JDBC driver property: transactionMode. <b>explicit</b> explicit <b>implicit</b> implicit
truncateFractionalSeconds	boolean		JDBC driver property: truncateFractionalSeconds.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
useServerSideUpdatableCursors	boolean		JDBC driver property: useServerSideUpdatableCursors.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
validateServerCertificate	boolean		JDBC driver property: validateServerCertificate.

**databaseStore > dataSource > properties.db2.i.native**

Data source properties for the IBM DB2 for i Native JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>read only</li> <li>all</li> <li>read call</li> </ul>	all	JDBC driver property: access. <b>read only</b> read only <b>all</b> all <b>read call</b> read call

Attribute name	Data type	Default value	Description
autoCommit	boolean	true	JDBC driver property: autoCommit.
batchStyle	<ul style="list-style-type: none"> <li>• 2.1</li> <li>• 2.0</li> </ul>	2.0	JDBC driver property: batchStyle. <b>2.1</b> 2.1 <b>2.0</b> 2.0
behaviorOverride	int		JDBC driver property: behaviorOverride.
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive
dataTruncation	string	true	JDBC driver property: dataTruncation.
databaseName	string	*LOCAL	JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy
dateSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		JDBC driver property: dateSeparator. <b>\,</b> The comma character (,). <b>b</b> The character b <b>.</b> The period character (.). <b>/</b> The forward slash character (/). <b>-</b> The dash character (-).
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		JDBC driver property: decimalSeparator. <b>\,</b> The comma character (,). <b>.</b> The period character (.).
directMap	boolean	true	JDBC driver property: directMap.
doEscapeProcessing	boolean	true	JDBC driver property: doEscapeProcessing.
fullErrors	boolean		JDBC driver property: fullErrors.
libraries	string		JDBC driver property: libraries.
lobThreshold	int Maximum: 500000	0	JDBC driver property: lobThreshold.

Attribute name	Data type	Default value	Description
lockTimeout	A period of time with second precision	0	JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>• 31</li> <li>• 63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 63
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
networkProtocol	int		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
prefetch	boolean	true	JDBC driver property: prefetch.
queryOptimizeGoal	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>	2	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).  <b>2</b> *ALLIO <b>1</b> *FIRSTIO

Attribute name	Data type	Default value	Description
reuseObjects	boolean	true	JDBC driver property: reuseObjects.
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
systemNaming	boolean	false	JDBC driver property: systemNaming.
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat.  <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  \, The comma character (,). <b>b</b> The character b : The colon character (:). . The period character (.).
trace	boolean		JDBC driver property: trace.
transactionTimeout	A period of time with second precision	0	JDBC driver property: transactionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateHex	<ul style="list-style-type: none"> <li>• binary</li> <li>• character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
useBlockInsert	boolean	false	JDBC driver property: useBlockInsert.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**databaseStore > dataSource > properties.db2.i.toolbox**

Data source properties for the IBM DB2 for i Toolbox JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>• read only</li> <li>• all</li> <li>• read call</li> </ul>	all	JDBC driver property: access. <b>read only</b> read only <b>all</b> all <b>read call</b> read call
behaviorOverride	int		JDBC driver property: behaviorOverride.
bidiImplicitReordering	boolean	true	JDBC driver property: bidiImplicitReordering.
bidiNumericOrdering	boolean	false	JDBC driver property: bidiNumericOrdering.
bidiStringType	int		JDBC driver property: bidiStringType.
bigDecimal	boolean	true	JDBC driver property: bigDecimal.
blockCriteria	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>	2	JDBC driver property: blockCriteria. Values are: 0 (no record blocking), 1 (block if FOR FETCH ONLY is specified), 2 (block if FOR UPDATE is specified).  <b>2</b> 2  <b>1</b> 1  <b>0</b> 0

Attribute name	Data type	Default value	Description
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> <li>• insensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive <b>insensitive</b> insensitive
dataCompression	boolean	true	JDBC driver property: dataCompression.
dataTruncation	boolean	true	JDBC driver property: dataTruncation.
databaseName	string		JDBC driver property: databaseName.
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy

Attribute name	Data type	Default value	Description
dateSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		<p>JDBC driver property: dateSeparator.</p> <p>The space character ( ).</p> <p>\, The comma character (,).</p> <p>. The period character (.).</p> <p>/ The forward slash character (/).</p> <p>- The dash character (-).</p>
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		<p>JDBC driver property: decimalSeparator.</p> <p>\, The comma character (,).</p> <p>. The period character (.).</p>
driver	<ul style="list-style-type: none"> <li>• toolbox</li> <li>• native</li> </ul>	toolbox	<p>JDBC driver property: driver.</p> <p><b>toolbox</b> toolbox</p> <p><b>native</b> native</p>
errors	<ul style="list-style-type: none"> <li>• full</li> <li>• basic</li> </ul>	basic	<p>JDBC driver property: errors.</p> <p><b>full</b> full</p> <p><b>basic</b> basic</p>
extendedDynamic	boolean	false	JDBC driver property: extendedDynamic.
extendedMetaData	boolean	false	JDBC driver property: extendedMetaData.
fullOpen	boolean	false	JDBC driver property: fullOpen.
holdInputLocators	boolean	true	JDBC driver property: holdInputLocators.
holdStatements	boolean	false	JDBC driver property: holdStatements.
isolationLevelSwitchingSupport	boolean	false	JDBC driver property: isolationLevelSwitchingSupport.
keepAlive	boolean		JDBC driver property: keepAlive.
lazyClose	boolean	false	JDBC driver property: lazyClose.
libraries	string		JDBC driver property: libraries.

Attribute name	Data type	Default value	Description
lobThreshold	int Minimum: 0 Maximum: 16777216	0	JDBC driver property: lobThreshold.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>31</li> <li>63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 64
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
metaDataSource	int Minimum: 0 Maximum: 1	1	JDBC driver property: metaDataSource.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
naming	<ul style="list-style-type: none"> <li>system</li> <li>sql</li> </ul>	sql	JDBC driver property: naming.  <b>system</b> system <b>sql</b> sql
package	string		JDBC driver property: package.
packageAdd	boolean	true	JDBC driver property: packageAdd.
packageCCSID	<ul style="list-style-type: none"> <li>13488</li> <li>1200</li> </ul>	13488	JDBC driver property: packageCCSID. Values are: 1200 (UCS-2) or 13488 (UTF-16).  <b>13488</b> 13488 (UTF-16) <b>1200</b> 1200 (UCS-2)
packageCache	boolean	false	JDBC driver property: packageCache.

Attribute name	Data type	Default value	Description
packageCriteria	<ul style="list-style-type: none"> <li>default</li> <li>select</li> </ul>	default	JDBC driver property: packageCriteria. <b>default</b> default <b>select</b> select
packageError	<ul style="list-style-type: none"> <li>exception</li> <li>none</li> <li>warning</li> </ul>	warning	JDBC driver property: packageError. <b>exception</b> exception <b>none</b> none <b>warning</b> warning
packageLibrary	string	QGPL	JDBC driver property: packageLibrary.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
prefetch	boolean	true	JDBC driver property: prefetch.
prompt	boolean	false	JDBC driver property: prompt.
proxyServer	string		JDBC driver property: proxyServer.
qaqqiniLibrary	string		JDBC driver property: qaqqiniLibrary.
queryOptimizeGoal	int Minimum: 0 Maximum: 2	0	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).
receiveBufferSize	int Minimum: 1		JDBC driver property: receiveBufferSize.
remarks	<ul style="list-style-type: none"> <li>system</li> <li>sql</li> </ul>	system	JDBC driver property: remarks. <b>system</b> system <b>sql</b> sql
rollbackCursorHold	boolean	false	JDBC driver property: rollbackCursorHold.
savePasswordWhenSerialized	boolean	false	JDBC driver property: savePasswordWhenSerialized.
secondaryUrl	string		JDBC driver property: secondaryUrl.
secure	boolean	false	JDBC driver property: secure.
sendBufferSize	int Minimum: 1		JDBC driver property: sendBufferSize.

Attribute name	Data type	Default value	Description
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
soLinger	A period of time with second precision		JDBC driver property: soLinger. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
soTimeout	A period of time with millisecond precision		JDBC driver property: soTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
sort	<ul style="list-style-type: none"> <li>• hex</li> <li>• table</li> <li>• language</li> </ul>	hex	JDBC driver property: sort. <b>hex</b> hex <b>table</b> table <b>language</b> language
sortLanguage	string		JDBC driver property: sortLanguage.
sortTable	string		JDBC driver property: sortTable.
sortWeight	<ul style="list-style-type: none"> <li>• unqiue</li> <li>• shared</li> </ul>		JDBC driver property: sortWeight. <b>unqiue</b> unique <b>shared</b> shared
tcpNoDelay	boolean		JDBC driver property: tcpNoDelay.
threadUsed	boolean	true	JDBC driver property: threadUsed.

Attribute name	Data type	Default value	Description
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat. <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  The space character ( ). \, The comma character (,). : The colon character (:). . The period character (.).
toolboxTrace	<ul style="list-style-type: none"> <li>• diagnostic</li> <li>• information</li> <li>• conversion</li> <li>• error</li> <li>• thread</li> <li>• proxy</li> <li>• none</li> <li>• datastream</li> <li>• pcml</li> <li>• all</li> <li>• jdbc</li> <li>• warning</li> </ul>		JDBC driver property: toolboxTrace. <b>diagnostic</b> diagnostic <b>information</b> information <b>conversion</b> conversion <b>error</b> error <b>thread</b> thread <b>proxy</b> proxy <b>none</b> none <b>datastream</b> datastream <b>pcml</b> pcml <b>all</b> all <b>jdbc</b> jdbc <b>warning</b> warning
trace	boolean		JDBC driver property: trace.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateBoolean	boolean	true	JDBC driver property: translateBoolean.

Attribute name	Data type	Default value	Description
translateHex	<ul style="list-style-type: none"> <li>binary</li> <li>character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
trueAutoCommit	boolean	false	JDBC driver property: trueAutoCommit.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaLooselyCoupledSupport	int  Minimum: 0  Maximum: 1	0	JDBC driver property: xaLooselyCoupledSupport.

**databaseStore > dataSource > properties.db2.jcc**

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for DB2.

false

Attribute name	Data type	Default value	Description
activateDatabase	int		JDBC driver property: activateDatabase.
alternateGroupDatabaseName	string		JDBC driver property: alternateGroupDatabaseName.
alternateGroupPortNumber	string		JDBC driver property: alternateGroupPortNumber.
alternateGroupServerName	string		JDBC driver property: alternateGroupServerName.
blockingReadConnectionTimeout	A period of time with second precision		JDBC driver property: blockingReadConnectionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
clientAccountingInformation	string		JDBC driver property: clientAccountingInformation.
clientApplicationInformation	string		JDBC driver property: clientApplicationInformation.
clientRerouteAlternatePortNumber	string		JDBC driver property: clientRerouteAlternatePortNumber.
clientRerouteAlternateServerName	string		JDBC driver property: clientRerouteAlternateServerName.

Attribute name	Data type	Default value	Description
clientUser	string		JDBC driver property: clientUser.
clientWorkstation	string		JDBC driver property: clientWorkstation.
connectionCloseWithInFlightTransaction	Transaction • 1		JDBC driver property: connectionCloseWithInFlightTransaction. 2 CONNECTION_CLOSE_WITH_ROLLBACK 1 CONNECTION_CLOSE_WITH_EXCEPTION
currentAlternateGroupEntry	int		JDBC driver property: currentAlternateGroupEntry.
currentFunctionPath	string		JDBC driver property: currentFunctionPath.
currentLocaleLcCtype	string		JDBC driver property: currentLocaleLcCtype.
currentLockTimeout	A period of time with second precision		JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
currentPackagePath	string		JDBC driver property: currentPackagePath.
currentPackageSet	string		JDBC driver property: currentPackageSet.
currentSQLID	string		JDBC driver property: currentSQLID.
currentSchema	string		JDBC driver property: currentSchema.
cursorSensitivity	• 2 • 1 • 0		JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). 2 TYPE_SCROLL_ASENSITIVE 1 TYPE_SCROLL_SENSITIVE_DYNAMIC 0 TYPE_SCROLL_SENSITIVE_STATIC
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean	true	JDBC driver property: deferPrepares.

Attribute name	Data type	Default value	Description
driverType	<ul style="list-style-type: none"> <li>2</li> <li>4</li> </ul>	4	JDBC driver property: driverType. 2 Type 2 JDBC driver. 4 Type 4 JDBC driver.
enableAlternateGroupSeamlessACR	boolean		JDBC driver property: enableAlternateGroupSeamlessACR.
enableClientAffinitiesList	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableClientAffinitiesList. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableExtendedDescribe	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedDescribe. 2 NO 1 YES
enableExtendedIndicators	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedIndicators. 2 NO 1 YES
enableNamedParameterMarkers	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSeamlessFailover	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeInputStreams	boolean		JDBC driver property: fullyMaterializeInputStreams.
fullyMaterializeInputStreamsOnBatchExecution	<ul style="list-style-type: none"> <li>1</li> </ul>		JDBC driver property: fullyMaterializeInputStreamsOnBatchExecution. 2 NO 1 YES
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.

Attribute name	Data type	Default value	Description
implicitRollbackOption	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: implicitRollbackOption.</p> <p>2 IMPLICIT_ROLLBACK_OPTION_N 1 IMPLICIT_ROLLBACK_OPTION_N 0 IMPLICIT_ROLLBACK_OPTION_N</p>
interruptProcessingMode	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: interruptProcessingMode.</p> <p>2 INTERRUPT_PROCESSING_MODI 1 INTERRUPT_PROCESSING_MODI 0 INTERRUPT_PROCESSING_MODI</p>
keepAliveTimeOut	A period of time with second precision		<p>JDBC driver property: keepAliveTimeOut. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
keepDynamic	int		JDBC driver property: keepDynamic.
kerberosServerPrincipal	string		JDBC driver property: kerberosServerPrincipal.
loginTimeout	A period of time with second precision		<p>JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
maxConnCachedParamBufferSize	int		JDBC driver property: maxConnCachedParamBufferSize.
maxRetriesForClientReroute	int		JDBC driver property: maxRetriesForClientReroute.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	50000	Port on which to obtain database connections.
profileName	string		JDBC driver property: profileName.

Attribute name	Data type	Default value	Description
queryCloseImplicit	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: queryCloseImplicit. Values are: 1 (QUERY_CLOSE_IMPLICIT_YES) or 2 (QUERY_CLOSE_IMPLICIT_NO).</p> <p>2        QUERY_CLOSE_IMPLICIT_NO 1        QUERY_CLOSE_IMPLICIT_YES</p>
queryDataSize	<p>int</p> <p>Minimum: 4096</p> <p>Maximum: 65535</p>		JDBC driver property: queryDataSize.
queryTimeoutInterruptProcessingMode	<p>int</p> <ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: queryTimeoutInterruptProcessingMode.</p> <p>2        INTERRUPT_PROCESSING_MODE_C 1        INTERRUPT_PROCESSING_MODE_S</p>
readOnly	boolean		JDBC driver property: readOnly.
recordTemporalHistory	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: recordTemporalHistory.</p> <p>2        NO 1        YES</p>
resultSetHoldability	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2        CLOSE_CURSORS_AT_COMMIT 1        HOLD_CURSORS_OVER_COMMIT</p>
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2        CLOSE_CURSORS_AT_COMMIT 1        HOLD_CURSORS_OVER_COMMIT</p>
retrieveMessagesFromServerOnGetMessage	boolean	true	JDBC driver property: retrieveMessagesFromServerOnGetMessage.

Attribute name	Data type	Default value	Description
retryIntervalForClientReroute	A period of time with second precision		JDBC driver property: retryIntervalForClientReroute. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 18</li> <li>• 15</li> <li>• 9</li> <li>• 16</li> <li>• 13</li> <li>• 11</li> <li>• 12</li> </ul>		<p>JDBC driver property: securityMechanism. Values are:</p> <ul style="list-style-type: none"> <li>3 (CLEAR_TEXT_PASSWORD_SECURITY),</li> <li>4 (USER_ONLY_SECURITY),</li> <li>7 (ENCRYPTED_PASSWORD_SECURITY),</li> <li>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY),</li> <li>11 (KERBEROS_SECURITY),</li> <li>12 (ENCRYPTED_USER_AND_DATA_SECURITY),</li> <li>13 (ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY),</li> <li>15 (PLUGIN_SECURITY),</li> <li>16 (ENCRYPTED_USER_ONLY_SECURITY),</li> <li>18 (TLS_CLIENT_CERTIFICATE_SECURITY).</li> </ul> <p>3 CLEAR_TEXT_PASSWORD_SECURITY  7 ENCRYPTED_PASSWORD_SECURITY  4 USER_ONLY_SECURITY  18 TLS_CLIENT_CERTIFICATE_SECURITY  15 PLUGIN_SECURITY  9 ENCRYPTED_USER_AND_PASSWORD_SECURITY  16 ENCRYPTED_USER_ONLY_SECURITY  13 ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY  11 KERBEROS_SECURITY  12 ENCRYPTED_USER_AND_DATA_SECURITY</p>
sendDataAsIs	boolean		JDBC driver property: sendDataAsIs.
serverName	string	localhost	Server where the database is running.
sessionTimeZone	string		JDBC driver property: sessionTimeZone.
sqljCloseStmtsWithOpenResultSet	boolean		JDBC driver property: sqljCloseStmtsWithOpenResultSet.

Attribute name	Data type	Default value	Description
sqljEnableClassLoaderSpecificProfiles	boolean		JDBC driver property: sqljEnableClassLoaderSpecificProfiles.
sslConnection	boolean		JDBC driver property: sslConnection.
streamBufferSize	int		JDBC driver property: streamBufferSize.
stripTrailingZerosForDecimalNumbers	Numbers <ul style="list-style-type: none"> <li>1</li> </ul>		JDBC driver property: stripTrailingZerosForDecimalNumbers. 2 NO 1 YES
sysSchema	string		JDBC driver property: sysSchema.
timerLevelForQueryTimeOut	<ul style="list-style-type: none"> <li>2</li> <li>1</li> <li>-1</li> </ul>		JDBC driver property: timerLevelForQueryTimeOut. 2 QUERYTIMEOUT_CONNECTION_LEVEL 1 QUERYTIMEOUT_STATEMENT_LEVEL -1 QUERYTIMEOUT_DISABLED
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceFileCount	int		JDBC driver property: traceFileCount.
traceFileSize	int		JDBC driver property: traceFileSize.
traceLevel	int	0	Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
traceOption	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: traceOption 1 1 0 0

Attribute name	Data type	Default value	Description
translateForBitData	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: translateForBitData. 2 SERVER_ENCODING_REPRESENTATION 1 HEX_REPRESENTATION
updateCountForBatch	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: updateCountForBatch. 2 TOTAL_UPDATE_COUNT 1 NO_UPDATE_COUNT
useCachedCursor	boolean		JDBC driver property: useCachedCursor.
useIdentityValLocalForAutoGeneratedKeys	boolean		JDBC driver property: useIdentityValLocalForAutoGeneratedKeys.
useJDBC41DefinitionForGetColumns	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC41DefinitionForGetColumns. 2 NO 1 YES
useJDBC4ColumnNameAndLabelSemantics	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
useTransactionRedirect	boolean		JDBC driver property: useTransactionRedirect.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaNetworkOptimization	boolean		JDBC driver property: xaNetworkOptimization.

**databaseStore > dataSource > properties.derby.client**

Data source properties for Derby Network Client JDBC driver.

false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1527	Port on which to obtain database connections.
retrieveMessageText	boolean	true	JDBC driver property: retrieveMessageText.
securityMechanism	<ul style="list-style-type: none"> <li>3</li> <li>7</li> <li>4</li> <li>9</li> <li>8</li> </ul>	3	<p>JDBC driver property: securityMechanism. Values are:</p> <p>3 (CLEAR_TEXT_PASSWORD_SECURITY),</p> <p>4 (USER_ONLY_SECURITY),</p> <p>7 (ENCRYPTED_PASSWORD_SECURITY),</p> <p>8 (STRONG_PASSWORD_SUBSTITUTE_SECURITY),</p> <p>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY)</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY</p> <p>7 ENCRYPTED_PASSWORD_SECURITY</p> <p>4 USER_ONLY_SECURITY</p> <p>9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p> <p>8 STRONG_PASSWORD_SUBSTITUTE_SECURITY</p>

Attribute name	Data type	Default value	Description
serverName	string	localhost	Server where the database is running.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		JDBC driver property: shutdownDatabase. <b>false</b> Do not shut down the database. <b>shutdown</b> Shut down the database when a connection is attempted.
ssl	<ul style="list-style-type: none"> <li>basic</li> <li>off</li> <li>peerAuthentication</li> </ul>		JDBC driver property: ssl. <b>basic</b> basic <b>off</b> off <b>peerAuthentication</b> peerAuthentication
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_XA_CALLS=2048, TRACE_ALL=-1.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**databaseStore > dataSource > properties.derby.embedded**  
 Data source properties for Derby Embedded JDBC driver.  
 false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		<p>JDBC driver property: shutdownDatabase.</p> <p><b>false</b> Do not shut down the database.</p> <p><b>shutdown</b> Shut down the database when a connection is attempted.</p>
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**databaseStore > dataSource > properties.informix**

Data source properties for the Informix JDBC driver.

false

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
ifxCLIENT_LOCALE	string		JDBC driver property: ifxCLIENT_LOCALE.
ifxCPMAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMInitPoolSize	int		JDBC driver property: ifxCPMInitPoolSize.
ifxCPMMaxConnections	int		JDBC driver property: ifxCPMMaxConnections.
ifxCPMMaxPoolSize	int		JDBC driver property: ifxCPMMaxPoolSize.
ifxCPMMinAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMMinAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMMinPoolSize	int		JDBC driver property: ifxCPMMinPoolSize.
ifxCPMServiceInterval	A period of time with millisecond precision		JDBC driver property: ifxCPMServiceInterval. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxDBANSIWARN	boolean		JDBC driver property: ifxDBANSIWARN.
ifxDBCENTURY	string		JDBC driver property: ifxDBCENTURY.
ifxDBDATE	string		JDBC driver property: ifxDBDATE.
ifxDBSPACETEMP	string		JDBC driver property: ifxDBSPACETEMP.

Attribute name	Data type	Default value	Description
ifxDBTEMP	string		JDBC driver property: ifxDBTEMP.
ifxDBTIME	string		JDBC driver property: ifxDBTIME.
ifxDBUPSPACE	string		JDBC driver property: ifxDBUPSPACE.
ifxDB_LOCALE	string		JDBC driver property: ifxDB_LOCALE.
ifxDELIMIDENT	boolean		JDBC driver property: ifxDELIMIDENT.
ifxENABLE_TYPE_CACHE	boolean		JDBC driver property: ifxENABLE_TYPE_CACHE.
ifxFET_BUF_SIZE	int		JDBC driver property: ifxFET_BUF_SIZE.
ifxGL_DATE	string		JDBC driver property: ifxGL_DATE.
ifxGL_DATETIME	string		JDBC driver property: ifxGL_DATETIME.
ifxIFXHOST	string	localhost	JDBC driver property: ifxIFXHOST.
ifxIFX_AUTOFREE	boolean		JDBC driver property: ifxIFX_AUTOFREE.
ifxIFX_DIRECTIVES	string		JDBC driver property: ifxIFX_DIRECTIVES.
ifxIFX_LOCK_MODE_WAIT	A period of time with second precision	2s	JDBC driver property: ifxIFX_LOCK_MODE_WAIT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxIFX_SOC_TIMEOUT	A period of time with millisecond precision		JDBC driver property: ifxIFX_SOC_TIMEOUT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxIFX_USEPUT	boolean		JDBC driver property: ifxIFX_USEPUT.

Attribute name	Data type	Default value	Description
ifxIFX_USE_STRENC	boolean		JDBC driver property: ifxIFX_USE_STRENC.
ifxIFX_XASPEC	string	y	JDBC driver property: ifxIFX_XASPEC.
ifxINFORMIXCONRETRY	int		JDBC driver property: ifxINFORMIXCONRETRY.
ifxINFORMIXCONTIME	A period of time with second precision		JDBC driver property: ifxINFORMIXCONTIME. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxINFORMIXOPCACHE	string		JDBC driver property: ifxINFORMIXOPCACHE.
ifxINFORMIXSTACKSIZE	int		JDBC driver property: ifxINFORMIXSTACKSIZE.
ifxJDBCTEMP	string		JDBC driver property: ifxJDBCTEMP.
ifxLDAP_IFXBASE	string		JDBC driver property: ifxLDAP_IFXBASE.
ifxLDAP_PASSWD	string		JDBC driver property: ifxLDAP_PASSWD.
ifxLDAP_URL	string		JDBC driver property: ifxLDAP_URL.
ifxLDAP_USER	string		JDBC driver property: ifxLDAP_USER.
ifxLOBCACHE	int		JDBC driver property: ifxLOBCACHE.
ifxNEWCODESET	string		JDBC driver property: ifxNEWCODESET.
ifxNEWLOCALE	string		JDBC driver property: ifxNEWLOCALE.
ifxNODEFDAC	string		JDBC driver property: ifxNODEFDAC.
ifxOPTCOMPIND	string		JDBC driver property: ifxOPTCOMPIND.
ifxOPTOFC	string		JDBC driver property: ifxOPTOFC.
ifxOPT_GOAL	string		JDBC driver property: ifxOPT_GOAL.
ifxPATH	string		JDBC driver property: ifxPATH.
ifxPDQPRIORITY	string		JDBC driver property: ifxPDQPRIORITY.

Attribute name	Data type	Default value	Description
ifxPLCONFIG	string		JDBC driver property: ifxPLCONFIG.
ifxPLOAD_LO_PATH	string		JDBC driver property: ifxPLOAD_LO_PATH.
ifxPROTOCOLTRACE	int		JDBC driver property: ifxPROTOCOLTRACE.
ifxPROTOCOLTRACEFILE	string		JDBC driver property: ifxPROTOCOLTRACEFILE.
ifxPROXY	string		JDBC driver property: ifxPROXY.
ifxPSORT_DBTEMP	string		JDBC driver property: ifxPSORT_DBTEMP.
ifxPSORT_NPROCS	boolean		JDBC driver property: ifxPSORT_NPROCS.
ifxSECURITY	string		JDBC driver property: ifxSECURITY.
ifxSQLH_FILE	string		JDBC driver property: ifxSQLH_FILE.
ifxSQLH_LOC	string		JDBC driver property: ifxSQLH_LOC.
ifxSQLH_TYPE	string		JDBC driver property: ifxSQLH_TYPE.
ifxSSLCONNECTION	string		JDBC driver property: ifxSSLCONNECTION.
ifxSTMT_CACHE	string		JDBC driver property: ifxSTMT_CACHE.
ifxTRACE	int		JDBC driver property: ifxTRACE.
ifxTRACEFILE	string		JDBC driver property: ifxTRACEFILE.
ifxTRUSTED_CONTEXT	string		JDBC driver property: ifxTRUSTED_CONTEXT.
ifxUSEV5SERVER	boolean		JDBC driver property: ifxUSEV5SERVER.
ifxUSE_DTENV	boolean		JDBC driver property: ifxUSE_DTENV.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
roleName	string		JDBC driver property: roleName.
serverName	string		Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**databaseStore > dataSource > properties.informix.jcc**

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for Informix.

false

Attribute name	Data type	Default value	Description
DBANSIWARN	boolean		JDBC driver property: DBANSIWARN.
DBDATE	string		JDBC driver property: DBDATE.
DBPATH	string		JDBC driver property: DBPATH.
DBSPACETEMP	string		JDBC driver property: DBSPACETEMP.
DBTEMP	string		JDBC driver property: DBTEMP.
DBUPSPACE	string		JDBC driver property: DBUPSPACE.
DELIMIDENT	boolean		JDBC driver property: DELIMIDENT.
IFX_DIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_DIRECTIVES. ON ON OFF OFF
IFX_EXTDIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_EXTDIRECTIVES. ON ON OFF OFF
IFX_UPDESC	string		JDBC driver property: IFX_UPDESC.

Attribute name	Data type	Default value	Description
IFX_XASTDCOMPLIANCE_XAEND	<ul style="list-style-type: none"> <li>0</li> </ul>		JDBC driver property: IFX_XASTDCOMPLIANCE_XAEND. <b>1</b> 1 <b>0</b> 0
INFORMIXOPCACHE	string		JDBC driver property: INFORMIXOPCACHE.
INFORMIXSTACKSIZE	string		JDBC driver property: INFORMIXSTACKSIZE.
NODEFDAC	<ul style="list-style-type: none"> <li>yes</li> <li>no</li> </ul>		JDBC driver property: NODEFDAC. <b>yes</b> yes <b>no</b> no
OPTCOMPIND	<ul style="list-style-type: none"> <li>2</li> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTCOMPIND. <b>2</b> 2 <b>1</b> 1 <b>0</b> 0
OPTOFC	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTOFC. <b>1</b> 1 <b>0</b> 0
PDQPRIORITY	<ul style="list-style-type: none"> <li>HIGH</li> <li>LOW</li> <li>OFF</li> </ul>		JDBC driver property: PDQPRIORITY. <b>HIGH</b> HIGH <b>LOW</b> LOW <b>OFF</b> OFF
PSORT_DBTEMP	string		JDBC driver property: PSORT_DBTEMP.
PSORT_NPROCS	string Maximum: 10		JDBC driver property: PSORT_NPROCS.
STMT_CACHE	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: STMT_CACHE. <b>1</b> 1 <b>0</b> 0
currentLockTimeout	A period of time with second precision	2s	JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean		JDBC driver property: deferPrepares.
driverType	int	4	JDBC driver property: driverType.
enableNamedParameterMarkers	int		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO).
enableSeamlessFailover	int		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO).
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.
keepDynamic	int		JDBC driver property: keepDynamic.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
progressiveStreaming	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		JDBC driver property: progressiveStreaming. Values are: 1 (YES) or 2 (NO).  2      NO 1      YES
queryDataSize	int  Minimum: 4096  Maximum: 10485760		JDBC driver property: queryDataSize.

Attribute name	Data type	Default value	Description
resultSetHoldability	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
retrieveMessagesFromServerOnGetMessage	boolean	true	JDBC driver property: retrieveMessagesFromServerOnGetMessage.
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 9</li> </ul>		<p>JDBC driver property: securityMechanism. Values are: 3 (CLEAR_TEXT_PASSWORD_SECURITY), 4 (USER_ONLY_SECURITY), 7 (ENCRYPTED_PASSWORD_SECURITY), 9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY).</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY 7 ENCRYPTED_PASSWORD_SECURITY 4 USER_ONLY_SECURITY 9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p>
serverName	string	localhost	Server where the database is running.
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.

Attribute name	Data type	Default value	Description
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
useJDBC4ColumnNameAndLabelSemantics	boolean		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO).
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**databaseStore > dataSource > properties.microsoft.sqlserver**  
Data source properties for Microsoft SQL Server JDBC Driver.

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database. Example: jdbc:sqlserver://localhost:1433;databaseName=myDB.
applicationIntent	<ul style="list-style-type: none"> <li>ReadOnly</li> <li>ReadWrite</li> </ul>		JDBC driver property: applicationIntent. <b>ReadOnly</b> ReadOnly <b>ReadWrite</b> ReadWrite
applicationName	string		JDBC driver property: applicationName.
authenticationScheme	<ul style="list-style-type: none"> <li>NativeAuthentication</li> <li>JavaKerberos</li> </ul>		JDBC driver property: authenticationScheme. <b>NativeAuthentication</b> NativeAuthentication <b>JavaKerberos</b> JavaKerberos

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
encrypt	boolean		JDBC driver property: encrypt.
failoverPartner	string		JDBC driver property: failoverPartner.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
instanceName	string		JDBC driver property: instanceName.
integratedSecurity	boolean		JDBC driver property: integratedSecurity.
lastUpdateCount	boolean		JDBC driver property: lastUpdateCount.
lockTimeout	A period of time with millisecond precision		JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
multiSubnetFailover	boolean		JDBC driver property: multiSubnetFailover.
packetSize	int Minimum: 512 Maximum: 32767		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.

Attribute name	Data type	Default value	Description
responseBuffering	<ul style="list-style-type: none"> <li>full</li> <li>adaptive</li> </ul>		JDBC driver property: responseBuffering. <b>full</b> full <b>adaptive</b> adaptive
selectMethod	<ul style="list-style-type: none"> <li>direct</li> <li>cursor</li> </ul>		JDBC driver property: selectMethod. <b>direct</b> direct <b>cursor</b> cursor
sendStringParametersAsUnicode	boolean	false	JDBC driver property: sendStringParametersAsUnicode.
sendTimeAsDatetime	boolean		JDBC driver property: sendTimeAsDatetime.
serverName	string	localhost	Server where the database is running.
trustServerCertificate	boolean		JDBC driver property: trustServerCertificate.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
workstationID	string		JDBC driver property: workstationID.
xopenStates	boolean		JDBC driver property: xopenStates.

#### databaseStore > dataSource > properties.oracle

Data source properties for Oracle JDBC driver.

false

Attribute name	Data type	Default value	Description
ONSConfiguration	string		JDBC driver property: ONSConfiguration.
TNSEntryName	string		JDBC driver property: TNSEntryName.
URL	string		URL for connecting to the database. Examples: jdbc:oracle:thin://localhost:1521/sample or jdbc:oracle:oci://localhost:1521/sample.
connectionProperties	string		JDBC driver property: connectionProperties.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
driverType	<ul style="list-style-type: none"> <li>oci</li> <li>thin</li> </ul>	thin	JDBC driver property: driverType.  <b>oci</b> oci <b>thin</b> thin
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	string		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1521	Port on which to obtain database connections.
serverName	string	localhost	Server where the database is running.
serviceName	string		JDBC driver property: serviceName.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**databaseStore > dataSource > properties.sybase**

Data source properties for Sybase JDBC driver.

false

Attribute name	Data type	Default value	Description
SERVER_INITIATED_TRANSACTIONS	<ul style="list-style-type: none"> <li>false</li> <li>true</li> </ul>	false	JDBC driver property: SERVER_INITIATED_TRANSACTIONS.  <b>false</b> false <b>true</b> true
connectionProperties	string	SELECT_OPENS_CURSOR=true	JDBC driver property: connectionProperties.
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	<ul style="list-style-type: none"> <li>• SSL</li> <li>• socket</li> </ul>		JDBC driver property: networkProtocol.  <b>SSL</b> SSL <b>socket</b> socket
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	5000	Port on which to obtain database connections.
resourceManagerName	string		JDBC driver property: resourceManagerName.
serverName	string	localhost	Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
version	int		JDBC driver property: version.

**databaseStore > dataSource > recoveryAuthData**

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

**grantType**

An access token grant type (as detailed in the OAuth specification) that is allowed for the provider. The equivalent provider parameter in the full application server profile is `oauth20.grant.types.allowed`.

false

string

**jwtGrantType**

The `grant_type` for JWT Token handler

false

Attribute name	Data type	Default value	Description
clockSkew	A period of time with second precision	300s	The time difference allowed between OpenID Connect Client and OpenID Connect Provider systems when they are not synchronized. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
iatRequired	boolean	false	The iat claim in a jwt token is required.
maxJtiCacheSize	long Minimum: 1	10000	The maximum size of cache, which keeps jti data of jwt token, to prevent the jti from being reused.
tokenMaxLifetime	A period of time with second precision	7200s	The time indicates the maximum lifetime of an alive jwt token since its issued-at-time. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**library**

Reference to shared library containing the mediator plugin class.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

### library > file

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

### library > fileset

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

### library > folder

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

### localStore

Clients are defined in server.xml and tokens are cached in the server.

false

Attribute name	Data type	Default value	Description
tokenStoreSize	long	2000	Token store size

### localStore > client

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
applicationType	<ul style="list-style-type: none"> <li>• native</li> <li>• web</li> </ul>	web	The type of application best describing the client. <b>native</b> native <b>web</b> web
displayname	string		Display name of the client.
enabled	boolean	true	Client is enabled if true, disabled if false.

Attribute name	Data type	Default value	Description
functionalUserId	string		A user identifier to be associated with access tokens obtained by this client using the client credentials grant type. When this client parameter is specified, the value is returned in the functional_user_id response parameter from the introspect endpoint.
id	string		A unique configuration ID.
introspectTokens	boolean	false	Boolean value specifying whether the client is allowed to access the introspection endpoint to introspect tokens issued by the authorization server.
name	string		Name of the client (sometimes referred to as the Id).
preAuthorizedScope	string		Space separated list of scope values that the client can use when requesting access tokens that are deemed to have been pre-approved by the resource owner and therefore does not require the resource owner's consent.
scope	string		Specify by spaces the list of scopes of the client.
secret	Reversably encoded password (string)		Secret key of the client.
sessionManaged	boolean	false	Boolean indicating whether the client participates in OpenID session management.
subjectType	<ul style="list-style-type: none"> <li>public</li> </ul>		Subject type requested for response to this client. <b>public</b> public
tokenEndpointAuthMethod	<ul style="list-style-type: none"> <li>client_secret_post</li> <li>none</li> <li>client_secret_basic</li> </ul>	client_secret_basic	The requested authentication method for the token endpoint of the client. <b>client_secret_post</b> client_secret_post <b>none</b> none <b>client_secret_basic</b> client_secret_basic

**localStore > client > functionalUserGroupIds**

A list of group ids to be associated with access tokens obtained by this client using the client credentials grant type. When this client parameter is specified, the value is returned in the functional\_user\_groupIds response parameter from the introspect endpoint.

false

string

**localStore > client > grantTypes**

Grant types the client may use.

false

**localStore > client > postLogoutRedirectUris**

Array of URLs supplied by the RP to which it may request that the end-user's user agent be redirected using the post\_logout\_redirect\_uri parameter after a logout has been performed.

false

string

**localStore > client > redirect**

Array of redirect URIs for use in redirect-based flows such as the authorization code and implicit grant types of the client. The first redirect URI is used as a default, when none is specified in a request.

false

string

**localStore > client > responseTypes**

Response types the client may use.

false

**mediatorClassname**

Mediator plugin class name. The equivalent provider parameter in the full application server profile is oauth20.mediator.classnames.

false

string

## OpenId Authentication (openId)

A variety of custom properties are available for OpenId authentication.

- authFilter
  - host
  - remoteAddress
  - requestUrl
  - userAgent
  - webApp
- userInfo

Attribute name	Data type	Default value	Description
authFilterRef	A reference to top level authFilter element (string).		Specifies the authentication filter reference.

Attribute name	Data type	Default value	Description
authenticationMode	<ul style="list-style-type: none"> <li>• checkid_immediate</li> <li>• checkid_setup</li> </ul>	checkid_setup	<p>Specifies the OpenID provider authentication mode either checkid_immediate or checkid_setup. checkid_setup is the default authentication mode.</p> <p><b>checkid_immediate</b> The checkid_immediate disables the browser interact with the user.</p> <p><b>checkid_setup</b> The checkid_setup enables the openID provider to interact with the user, to request authentication or self-registration before returning a result to the openId relying party.</p>
hashAlgorithm	<ul style="list-style-type: none"> <li>• SHA256</li> <li>• SHA1</li> </ul>	SHA256	<p>Specifies the hash algorithm that is used to sign and encrypt the OpenID provider response parameters.</p> <p><b>SHA256</b> Secure hash algorithm SHA256</p> <p><b>SHA1</b> Secure hash algorithm SHA1</p>
hostNameVerificationEnabled	boolean	true	Specifies whether enable host name verification or not.
httpsRequired	boolean	true	Require SSL communication between the OpenID relying party and provider service.
mapIdentityToRegistryUser	boolean	false	Specifies whether to map identity to registry user. The user registry is not used to create the user subject.
providerIdentifier	string		Specifies a default OpenID provider URL where users get the Open IDs.
realmIdentifier	string		Specifies the attribute for the OpenID provider name.

Attribute name	Data type	Default value	Description
sslRef	A reference to top level ssl element (string).		Specifies an ID of the SSL configuration is used to connect to the OpenID provider.
useClientIdentity	boolean	false	Specifies whether to use the client OpenID identity to create a user subject. If set to true, only the OpenID client identity is used. If set to false and the first element of userInfoRef is found, we use it to create a user subject. Otherwise, we use the OpenID identity to create a user subject.
userInfoRef	List of references to top level userInfo elements (comma-separated string).	email	Specifies a list of userInfo references separated by commas for the OpenID provider to include in the response.

#### **authFilter**

Specifies the authentication filter reference.

false

#### **authFilter > host**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
name	string		Specifies the name.

#### **authFilter > remoteAddress**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
ip	string		Specifies the IP address.

Attribute name	Data type	Default value	Description
matchType	<ul style="list-style-type: none"> <li>lessThan</li> <li>equals</li> <li>greaterThan</li> <li>contains</li> <li>notContain</li> </ul>	contains	Specifies the match type. <b>lessThan</b> Less than <b>equals</b> Equals <b>greaterThan</b> Greater than <b>contains</b> Contains <b>notContain</b> Not contain

**authFilter > requestUrl**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>equals</li> <li>contains</li> <li>notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
urlPattern	string		Specifies the URL pattern.

**authFilter > userAgent**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
agent	string		Specifies the user agent
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>equals</li> <li>contains</li> <li>notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain

**authFilter > webApp**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
name	string		Specifies the name.

### userInfo

Specifies a list of userInfo references separated by commas for the OpenID provider to include in the response.

false

Attribute name	Data type	Default value	Description
alias	string	email	Specifies an alias name.
count	int Minimum: 1	1	Specifies how much userInfo is included in the response of the openID provider.
id	string		A unique configuration ID.
required	boolean	true	Specifies whether user information is required or not.
uriType	string	http://axschema.org/contact/email	Specifies a URI type.

## OpenID Connect Client (openidConnectClient)

OpenID Connect client.

- audiences
- authFilter
  - host
  - remoteAddress
  - requestUrl
  - userAgent
  - webApp

Attribute name	Data type	Default value	Description
authFilterRef	A reference to top level authFilter element (string).		Specifies the authentication filter reference.
authnSessionDisabled	boolean	true	An authentication session cookie will not be created for inbound propagation. The client is expected to send a valid OAuth token for every request.
authorizationEndpointUrl	string		Specifies an Authorization end point URL.

Attribute name	Data type	Default value	Description
clientId	string		Identity of the client.
clientSecret	Reversably encoded password (string)		Secret key of the client.
createSession	boolean	true	Specifies whether to create an HttpSession if the current HttpSession does not exist.
disableIssChecking	boolean	false	Do not check for the issuer while validating the json response for inbound token propagation.
disableLtpaCookie	boolean	false	Do not create an LTPA Token during processing of the OAuth token. Create a cookie of the specific Service Provider instead.
grantType	<ul style="list-style-type: none"> <li>implicit</li> <li>authorization_code</li> </ul>	authorization_code	<p>Specifies the grant type to use for this client.</p> <p><b>implicit</b> Implicit grant type</p> <p><b>authorization_code</b> Authorization code grant type</p>
groupIdIdentifier	string	groupIds	Specifies a JSON attribute in the ID token that is used as the name of the group that the authenticated principal is a member of.
headerName	string		The name of the header which carries the inbound token in the request.
hostNameVerificationEnabled	boolean	false	Specifies whether to enable host name verification.
httpsRequired	boolean	true	Require SSL communication between the OpenID relying party and provider service.
id	string		A unique configuration ID.
inboundPropagation	<ul style="list-style-type: none"> <li>supported</li> <li>none</li> <li>required</li> </ul>	none	<p>Controls the operation of the token inbound propagation of the OpenID relying party.</p> <p><b>supported</b> Support inbound token propagation</p> <p><b>none</b> Do not support inbound token propagation</p> <p><b>required</b> Require inbound token propagation</p>

Attribute name	Data type	Default value	Description
includeIdTokenInSubject	boolean	true	Specifies whether to include ID token in the client subject.
initialStateCacheCapacity	int Minimum: 0	3000	Specifies the beginning capacity of state cache. The capacity grows bigger when needed by itself.
isClientSideRedirectSupported	boolean	true	Specifies whether the client supports redirect at client side.
issuerIdentifier	string		An Issuer Identifier is a case-sensitive URL using the HTTPS scheme that contains scheme, host and optionally port number and path components.
jwkEndpointUrl	string		Specifies a JWK end point URL.
mapIdentityToRegistryUser	boolean	false	Specifies whether to map the identity to a registry user. If this is set to false, then the user registry is not used to create the user subject.
nonceEnabled	boolean	false	Enable the nonce parameter in the authorization code flow.
reAuthnCushion	A period of time with millisecond precision	0s	The time period to authenticate a user again when its tokens are about to expire. The expiration time of an ID token is specified by its exp claim. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
reAuthnOnAccessTokenExpiration	boolean	true	Authenticate a user again when its authenticating access token expires and disableLtpaCookie is set to true.
realmIdentifier	string	realmName	Specifies a JSON attribute in the ID token that is used as the realm name.

Attribute name	Data type	Default value	Description
realmName	string		Specifies a realm name to be used to create the user subject when the mapIdentityToRegistryUser is set to false.
redirectToRPHostAndPort	string		Specifies a redirect OpenID relying party host and port number.
scope	tokenType	openid profile	OpenID Connect scope (as detailed in the OpenID Connect specification) that is allowed for the provider.
signatureAlgorithm	<ul style="list-style-type: none"> <li>• HS256</li> <li>• none</li> <li>• RS256</li> </ul>	HS256	<p>Specifies the signature algorithm that will be used to verify the signature of the ID token.</p> <p><b>HS256</b> Use the HS256 signature algorithm to sign and verify tokens</p> <p><b>none</b> Tokens are not required to be signed</p> <p><b>RS256</b> Use the RS256 signature algorithm to sign and verify tokens</p>
sslRef	A reference to top level ssl element (string).		Specifies an ID of the SSL configuration that is used to connect to the OpenID Connect provider.
tokenEndpointAuthMethod	<ul style="list-style-type: none"> <li>• post</li> <li>• basic</li> </ul>	post	<p>The method to use for sending credentials to the token endpoint of the OpenID Connect provider in order to authenticate the client.</p> <p><b>post</b> post</p> <p><b>basic</b> basic</p>
tokenEndpointUrl	string		Specifies a token end point URL.
trustAliasName	string		Key alias name to locate public key for signature validation with asymmetric algorithm.
trustStoreRef	A reference to top level keyStore element (string).		A keystore containing the public key necessary for verifying the signature of the ID token.

Attribute name	Data type	Default value	Description
uniqueUserIdentifier	string	uniqueSecurityName	Specifies a JSON attribute in the ID token that is used as the unique user name as it applies to the WSCredential in the subject.
userIdentifier	string		Specifies a JSON attribute in the ID token that is used as the user principal name in the subject. If no value is specified, the JSON attribute "sub" is used.
userIdentityToCreateSubject	string	sub	Specifies a user identity in the ID token used to create the user subject.
validationEndpointUrl	string		The endpoint URL for validating the token inbound propagation. The type of endpoint is decided by the validationMethod.
validationMethod	<ul style="list-style-type: none"> <li>• introspect</li> <li>• userinfo</li> </ul>	introspect	<p>The method of validation on the token inbound propagation.</p> <p><b>introspect</b> Validate inbound tokens using token introspection</p> <p><b>userinfo</b> Validate inbound tokens using the userinfo end point</p>

**audiences**

The trusted audience list that is verified against the aud claim in the JSON web token.

false

string

**authFilter**

Specifies the authentication filter reference.

false

**authFilter > host**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
name	string		Specifies the name.

#### **authFilter > remoteAddress**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
ip	string		Specifies the IP address.
matchType	<ul style="list-style-type: none"> <li>• lessThan</li> <li>• equals</li> <li>• greaterThan</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>lessThan</b> Less than <b>equals</b> Equals <b>greaterThan</b> Greater than <b>contains</b> Contains <b>notContain</b> Not contain

#### **authFilter > requestUrl**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
urlPattern	string		Specifies the URL pattern.

#### **authFilter > userAgent**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
agent	string		Specifies the user agent
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain

**authFilter > webApp**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
name	string		Specifies the name.

## OpenID Connect Server Provider (openidConnectProvider)

OpenID Connect server provider

- claimToUserRegistryMap
  - property
- customClaims
- discovery
  - claimsSupported
  - grantTypesSupported
  - idTokenSigningAlgValuesSupported
  - responseModesSupported
  - responseTypesSupported
  - scopesSupported
  - tokenEndpointAuthMethodsSupported
- oauthProvider
  - autoAuthorizeClient
  - databaseStore
    - dataSource
      - connectionManager
      - containerAuthData
      - jaasLoginContextEntry
      - jdbcDriver

- library
  - file
  - fileset
  - folder
- properties
- properties.datadirect.sqlserver
- properties.db2.i.native
- properties.db2.i.toolbox
- properties.db2.jcc
- properties.derby.client
- properties.derby.embedded
- properties.informix
- properties.informix.jcc
- properties.microsoft.sqlserver
- properties.oracle
- properties.sybase
- recoveryAuthData
- grantType
- jwtGrantType
- library
  - file
  - fileset
  - folder
- localStore
  - client
    - functionalUserGroupIds
    - grantTypes
    - postLogoutRedirectUris
    - redirect
    - responseTypes
- mediatorClassname
- scopeToClaimMap
  - property

Attribute name	Data type	Default value	Description
allowDefaultSsoCookieName	boolean	false	When this property is set to true, the default SSO cookie name, ltpaToken2, is used if a custom SSO cookie name is not configured. If a custom cookie name is configured for SSO, that cookie name is used. If a custom cookie name is not configured and this property is set to false, an auto-generated SSO cookie name will be used.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
idTokenLifetime	A period of time with second precision	2h	Time that ID token is valid (seconds). Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
issuerIdentifier	string		Specify an issuer identifier for the issuer of the response.
jwkEnabled	boolean	false	Enables or disables JWK.
jwkRotationTime	A period of time with minute precision	720m	Amount of time after which a new JWK will be generated. Specify a positive integer followed by a unit of time, which can be hours (h) or minutes (m). For example, specify 30 minutes as 30m. You can include multiple values in a single entry. For example, 1h30m is equivalent to 90 minutes.
jwkSigningKeySize	<ul style="list-style-type: none"> <li>• 4096</li> <li>• 1024</li> <li>• 2048</li> </ul>	2048	Size measured in bits of the signing key. <b>4096</b> 4096 bits <b>1024</b> 1024 bits <b>2048</b> 2048 bits
keyAliasName	string		Key alias name to locate the private key for signing with an asymmetric algorithm.
keyStoreRef	A reference to top level keyStore element (string).	opKeyStore	A keystore containing the private key necessary for signing with an asymmetric algorithm.
oauthProviderRef	A reference to top level oauthProvider element (string).		A reference to the ID of an OAuth provider.
sessionManaged	boolean	false	Indicate by true or false whether session management is supported. Default is false.

Attribute name	Data type	Default value	Description
signatureAlgorithm	<ul style="list-style-type: none"> <li>• HS256</li> <li>• none</li> <li>• RS256</li> </ul>	HS256	Specify the signature algorithm that will be used to sign the ID token.  <b>HS256</b> HMAC using SHA-256 hash  <b>none</b> No signature  <b>RS256</b> RSASSA-PKCS-v1_5 using SHA-256 hash
trustStoreRef	A reference to top level keyStore element (string).		A keystore containing the public key necessary for verifying a signature of the JWT token.

### claimToUserRegistryMap

Specify the user registry key for the claim.

false

Attribute name	Data type	Default value	Description
address	string	postalAddress	Specify the user registry key that will be retrieved for the address claim.
email	string	mail	Specify the user registry key that will be retrieved for the email claim.
given_name	string	givenName	Specify the user registry key that will be retrieved for the given_name claim.
name	string	displayName	Specify the user registry key that will be retrieved for the name claim.
phone_number	string	telephoneNumber	Specify the user registry key that will be retrieved for the phone_number claim.
picture	string	photoURL	Specify the user registry key that will be retrieved for the picture claim.

### claimToUserRegistryMap > property

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Specify the name of the property
value	string		Specify the value of the property

**customClaims**

The extra claims to be put in the payloads of the ID Token, in addition to the default realmName, uniqueSecurityName and groupIds claims.

false

string

**discovery**

Discovery is based on OpenID Connect and Jazz Authorization Server Profile.

false

Attribute name	Data type	Default value	Description
claimsParameterSupported	boolean	false	Indicate by true or false whether claims parameter is supported.
requestParameterSupported	boolean	false	Indicate by true or false whether request parameter is supported.
requestUriParameterSupported	boolean	false	Indicate by true or false whether request URI parameter is supported.
requireRequestUriRegistration	boolean	false	Indicate by true or false whether require request URI registration is supported.

**discovery > claimsSupported**

Specify by comma the list of claims that will be supported.

false

string

**discovery > grantTypesSupported**

Specify by comma the list of the grant types that will be used.

false

**discovery > idTokenSigningAlgValuesSupported**

Specify the signature algorithm that will be used to sign the ID token.

false

**discovery > responseModesSupported**

Specify by comma the list of the response modes that will be used.

false

**discovery > responseTypesSupported**

Specify by comma the list of the response types that will be supported by the OP.

false

**discovery > scopesSupported**

Specify by comma the list of scopes that will be supported.

false

string

**discovery > tokenEndpointAuthMethodsSupported**

Specify by comma the list of the token endpoint authentication methods that will be used.

false

**oauthProvider**

A reference to the ID of an OAuth provider.

false

Attribute name	Data type	Default value	Description
accessTokenLength	long	40	Length of the generated OAuth access token. The equivalent provider parameter in the full application server profile is <code>oauth20.access.token.length</code> .
accessTokenLifetime	A period of time with second precision	7200	Time that access token is valid (seconds). The equivalent provider parameter in the full application server profile is <code>oauth20.token.lifetime.seconds</code> . Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
allowPublicClients	boolean	false	A value of false disables the access of public clients as detailed in the OAuth specification. The equivalent provider parameter in the full application server profile is <code>oauth20.allow.public.clients</code> .
authorizationCodeLength	long	30	Length of the generated authorization code. The equivalent provider parameter in the full application server profile is <code>oauth20.code.length</code> .

Attribute name	Data type	Default value	Description
authorizationCodeLifetime	A period of time with second precision	60	Authorization code lifetime (seconds). The equivalent provider parameter in the full application server profile is <code>oauth20.code.lifetime.seconds</code> . Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
authorizationErrorTemplate	string		URL of a custom authorization error page template. The equivalent provider parameter in the full application server profile is <code>oauth20.authorization.error.template</code> .
authorizationFormTemplate	string	template.html	URL of a custom authorization page template. The equivalent provider parameter in the full application server profile is <code>oauth20.authorization.form.template</code> .
authorizationGrantLifetime	A period of time with second precision	604800	Authorization grant lifetime (seconds). The equivalent provider parameter in the full application server profile is <code>oauth20.max.authorization.grant.lifetime.seconds</code> . Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
autoAuthorize	boolean	false	To use auto authorization, append the <code>autoAuthorize</code> parameter to requests with a value of true. The equivalent provider parameter in the full application server profile is <code>oauth20.autoauthorize.param</code> .

Attribute name	Data type	Default value	Description
autoAuthorizeParam	string	autoauthz	To use auto authorization, append the autoAuthorize parameter to requests with a value of true. The equivalent provider parameter in the full application server profile is oauth20.autoauthorize.param.
certAuthentication	boolean	false	Enable the authentication of client certificate in the https request.
characterEncoding	string		Set request character encoding to this value. The equivalent provider parameter in the full application server profile is characterEncoding.
clientTokenCacheSize	long		Maximum number of entries in the client token cache.
clientURISubstitutions	string		Optional value to replace client URI strings for dynamic hostnames. The equivalent provider parameter in the full application server profile is oauth20.client.uri.substitutions.
consentCacheEntryLifetime	A period of time with second precision	1800	Time that an entry in the consent cache is valid (seconds). Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
consentCacheSize	long Minimum: 0	1000	Maximum number of entries allowed in the consent cache.
coverageMapSessionMaxAge	A period of time with second precision	600	The max-age value (seconds) for the cache-control header of the coverage map service. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
customLoginURL	string	login.jsp	URL of a custom login page. The equivalent provider parameter in the full application server profile is <code>oauth20.authorization.loginURL</code> .
filter	string		URI filter selects requests to be authorized by this provider. The equivalent provider parameter in the full application server profile is <code>Filter</code> .
httpsRequired	boolean	true	SSL communication between the OAuth client and provider is required.
includeTokenInSubject	boolean	true	If the value is true, add the <code>com.ibm.wsspi.security.oauth20.token.WSOAuth</code> as a private credential. The equivalent provider parameter in the full application server profile is <code>includeToken</code> .
issueRefreshToken	boolean	true	A value of false disables generation and the use of refresh tokens. The equivalent provider parameter in the full application server profile is <code>oauth20.issue.refresh.token</code> .
libraryRef	A reference to top level library element (string).		Reference to shared library containing the mediator plugin class.
oauthOnly	boolean	true	If the value is true, then requests matching the filter must have an access token or they will be failed. If false, then matching requests will be checked for other authentication data if no access token is present. The equivalent provider parameter in the full application server profile is <code>oauthOnly</code> .
refreshTokenLength	long	50	Length of generated refresh token. The equivalent provider parameter in the full application server profile is <code>oauth20.refresh.token.length</code> .
skipResourceOwnerValidation	boolean	false	If the value is true, skip validation of resource owner.
userClientTokenLimit	long		Token limit for each user and client combination.

**oauthProvider > autoAuthorizeClient**

Name of a client that is allowed to use auto authorization. The equivalent provider parameter in the full application server profile is `oauth20.autoauthorize.clients`.

false

string

**oauthProvider > databaseStore**

Clients are defined and tokens are cached in the database.

false

Attribute name	Data type	Default value	Description
<code>cleanupExpiredTokenInterval</code>	A period of time with second precision	3600	Expired token cleanup interval (seconds). The equivalent provider parameter in the full application server profile is <code>oauthjdbc.CleanupInterval</code> . Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
<code>dataSourceRef</code>	A reference to top level <code>dataSource</code> element (string).		Reference to the data source for the store.
<code>password</code>	Reversably encoded password (string)		Password used to access the database.
<code>schema</code>	string	<code>OAuthDBSchema</code>	Schema
<code>user</code>	string		User

**oauthProvider > databaseStore > dataSource**

Reference to the data source for the store.

false

Attribute name	Data type	Default value	Description
<code>beginTranForResultSetScrollingApps</code>	boolean	true	Attempt transaction enlistment when result set scrolling interfaces are used.
<code>beginTranForVendorAPIs</code>	boolean	true	Attempt transaction enlistment when vendor interfaces are used.

Attribute name	Data type	Default value	Description
commitOrRollbackOnCleanup	<ul style="list-style-type: none"> <li>• commit</li> <li>• rollback</li> </ul>		<p>Determines how to clean up connections that might be in a database unit of work (AutoCommit=false) when the connection is closed or returned to the pool.</p> <p><b>commit</b> Clean up the connection by committing.</p> <p><b>rollback</b> Clean up the connection by rolling back.</p>
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a data source.
connectionSharing	<ul style="list-style-type: none"> <li>• MatchOriginalRequest</li> <li>• MatchCurrentState</li> </ul>	MatchOriginalRequest	<p>Specifies how connections are matched for sharing.</p> <p><b>MatchOriginalRequest</b> When sharing connections, match based on the original connection request.</p> <p><b>MatchCurrentState</b> When sharing connections, match based on the current state of the connection.</p>
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

Attribute name	Data type	Default value	Description
enableConnectionCasting	boolean	false	Indicates that connections obtained from the data source should be castable to interface classes that the JDBC vendor connection implementation implements. Enabling this option incurs additional overhead on each getConnection operation. If vendor JDBC interfaces are needed less frequently, it might be more efficient to leave this option disabled and use Connection.unwrap(interface) only where it is needed.
isolationLevel	<ul style="list-style-type: none"> <li>• TRANSACTION_REPEATABLE_READ</li> <li>• TRANSACTION_READ_COMMITTED</li> <li>• TRANSACTION_SERIALIZABLE</li> <li>• TRANSACTION_READ_UNCOMMITTED</li> <li>• TRANSACTION_SNAPSHOT</li> </ul>		<p>Default transaction isolation level.</p> <p><b>TRANSACTION_REPEATABLE_READ</b> Dirty reads and non-repeatable reads are prevented; phantom reads can occur.</p> <p><b>TRANSACTION_READ_COMMITTED</b> Dirty reads are prevented; non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SERIALIZABLE</b> Dirty reads, non-repeatable reads and phantom reads are prevented.</p> <p><b>TRANSACTION_READ_UNCOMMITTED</b> Dirty reads, non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SNAPSHOT</b> Snapshot isolation for Microsoft SQL Server JDBC Driver and DataDirect Connect for JDBC driver.</p>

Attribute name	Data type	Default value	Description
jaasLoginContextEntryRef	A reference to top level jaasLoginContextEntry element (string).		JAAS login context entry for authentication.
jdbcDriverRef	A reference to top level jdbcDriver element (string).		JDBC driver for a data source.
jndiName	string		JNDI name for a data source.
queryTimeout	A period of time with second precision		Default query timeout for SQL statements. In a JTA transaction, syncQueryTimeoutWithTransactionTimeout can override this default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.
statementCacheSize	int Minimum: 0	10	Maximum number of cached statements per connection.
supplementalJDBCTrace	boolean		Supplements the JDBC driver trace that is logged when JDBC driver trace is enabled in bootstrap.properties. JDBC driver trace specifications include: com.ibm.ws.database.logwriter, com.ibm.ws.db2.logwriter, com.ibm.ws.derby.logwriter, com.ibm.ws.informix.logwriter, com.ibm.ws.oracle.logwriter, com.ibm.ws.sqlserver.logwriter, com.ibm.ws.sybase.logwriter
syncQueryTimeoutWithTransactionTimeout	boolean	false	Use the time remaining (if any) in a JTA transaction as the default query timeout for SQL statements.
transactional	boolean	true	Enable participation in transactions that are managed by the application server.

Attribute name	Data type	Default value	Description
type	<ul style="list-style-type: none"> <li>• javax.sql.DataSource</li> <li>• javax.sql.XADataSource</li> <li>• javax.sql.ConnectionPoolDataSource</li> </ul>		Type of data source. <b>javax.sql.DataSource</b> javax.sql.DataSource <b>javax.sql.XADataSource</b> javax.sql.XADataSource <b>javax.sql.ConnectionPoolDataSource</b> javax.sql.ConnectionPoolDataSource

**oauthProvider > databaseStore > dataSource > connectionManager**

Connection manager for a data source.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.

Attribute name	Data type	Default value	Description
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.

Attribute name	Data type	Default value	Description
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**oauthProvider > databaseStore > dataSource > containerAuthData**

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

**oauthProvider > databaseStore > dataSource > jaasLoginContextEntry**

JAAS login context entry for authentication.

false

Attribute name	Data type	Default value	Description
loginModuleRef	List of references to top level jaasLoginModule elements (comma-separated string).	hashtable,userNameAndPassword,certificateURL	Word certificateURL of a JAAS login module.
name	string		Name of a JAAS configuration entry.

**oauthProvider > databaseStore > dataSource > jdbcDriver**

JDBC driver for a data source.

false

Attribute name	Data type	Default value	Description
javax.sql.ConnectionPoolDataSource	string		JDBC driver implementation of javax.sql.ConnectionPoolDataSource.
javax.sql.DataSource	string		JDBC driver implementation of javax.sql.DataSource.
javax.sql.XADataSource	string		JDBC driver implementation of javax.sql.XADataSource.
libraryRef	A reference to top level library element (string).		Identifies JDBC driver JARs and native files.

**oauthProvider > databaseStore > dataSource > jdbcDriver > library**

Identifies JDBC driver JARs and native files.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

**oauthProvider > databaseStore > dataSource > jdbcDriver > library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**oauthProvider > databaseStore > dataSource > jdbcDriver > library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**oauthProvider > databaseStore > dataSource > jdbcDriver > library > folder**  
 Id of referenced folder  
 false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**oauthProvider > databaseStore > dataSource > properties**

List of JDBC vendor properties for the data source. For example, databaseName="dbname" serverName="localhost" portNumber="50000".

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database.
databaseName	string		JDBC driver property: databaseName.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
serverName	string		Server where the database is running.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**oauthProvider > databaseStore > dataSource > properties.datadirect.sqlserver**

Data source properties for the DataDirect Connect for JDBC driver for Microsoft SQL Server.

false

Attribute name	Data type	Default value	Description
JDBCBehavior	<ul style="list-style-type: none"> <li>• 1</li> <li>• 0</li> </ul>	0	JDBC driver property: JDBCBehavior. Values are: 0 (JDBC 4.0) or 1 (JDBC 3.0).  <b>1</b> JDBC 3.0 <b>0</b> JDBC 4.0
XATransactionGroup	string		JDBC driver property: XATransactionGroup.
XMLDescribeType	<ul style="list-style-type: none"> <li>• longvarbinary</li> <li>• longvarchar</li> </ul>		JDBC driver property: XMLDescribeType.  <b>longvarbinary</b> longvarbinary  <b>longvarchar</b> longvarchar
accountingInfo	string		JDBC driver property: accountingInfo.
alternateServers	string		JDBC driver property: alternateServers.
alwaysReportTriggerResults	boolean		JDBC driver property: alwaysReportTriggerResults.
applicationName	string		JDBC driver property: applicationName.
authenticationMethod	<ul style="list-style-type: none"> <li>• ntlm</li> <li>• userIdPassword</li> <li>• kerberos</li> <li>• auto</li> </ul>		JDBC driver property: authenticationMethod.  <b>ntlm</b> ntlm <b>userIdPassword</b> userIdPassword  <b>kerberos</b> kerberos  <b>auto</b> auto
bulkLoadBatchSize	long		JDBC driver property: bulkLoadBatchSize.
bulkLoadOptions	long		JDBC driver property: bulkLoadOptions.
clientHostName	string		JDBC driver property: clientHostName.

Attribute name	Data type	Default value	Description
clientUser	string		JDBC driver property: clientUser.
codePageOverride	string		JDBC driver property: codePageOverride.
connectionRetryCount	int		JDBC driver property: connectionRetryCount.
connectionRetryDelay	A period of time with second precision		JDBC driver property: connectionRetryDelay. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
convertNull	int		JDBC driver property: convertNull.
databaseName	string		JDBC driver property: databaseName.
dateTimeInputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeInputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
dateTimeOutputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeOutputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
describeInputParameters	<ul style="list-style-type: none"> <li>• describeIfString</li> <li>• noDescribe</li> <li>• describeIfDateTime</li> <li>• describeAll</li> </ul>		JDBC driver property: describeInputParameters.  <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll

Attribute name	Data type	Default value	Description
describeOutputParameters	<ul style="list-style-type: none"> <li>describeIfString</li> <li>noDescribe</li> <li>describeIfDateTime</li> <li>describeAll</li> </ul>		JDBC driver property: describeOutputParameters. <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll
enableBulkLoad	boolean		JDBC driver property: enableBulkLoad.
enableCancelTimeout	boolean		JDBC driver property: enableCancelTimeout.
encryptionMethod	<ul style="list-style-type: none"> <li>loginSSL</li> <li>requestSSL</li> <li>SSL</li> <li>noEncryption</li> </ul>		JDBC driver property: encryptionMethod. <b>loginSSL</b> loginSSL <b>requestSSL</b> requestSSL <b>SSL</b> SSL <b>noEncryption</b> noEncryption
failoverGranularity	<ul style="list-style-type: none"> <li>disableIntegrityCheck</li> <li>atomicWithRepositioning</li> <li>nonAtomic</li> <li>atomic</li> </ul>		JDBC driver property: failoverGranularity. <b>disableIntegrityCheck</b> disableIntegrityCheck <b>atomicWithRepositioning</b> atomicWithRepositioning <b>nonAtomic</b> nonAtomic <b>atomic</b> atomic
failoverMode	<ul style="list-style-type: none"> <li>connect</li> <li>select</li> <li>extended</li> </ul>		JDBC driver property: failoverMode. <b>connect</b> connect <b>select</b> select <b>extended</b> extended
failoverPreconnect	boolean		JDBC driver property: failoverPreconnect.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
initializationString	string		JDBC driver property: initializationString.
insensitiveResultSetBufferSize	int		JDBC driver property: insensitiveResultSetBufferSize.

Attribute name	Data type	Default value	Description
javaDoubleToString	boolean		JDBC driver property: javaDoubleToString.
loadBalancing	boolean		JDBC driver property: loadBalancing.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
longDataCacheSize	int Minimum: -1		JDBC driver property: longDataCacheSize.
netAddress	string		JDBC driver property: netAddress.
packetSize	int Minimum: -1 Maximum: 128		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
queryTimeout	A period of time with second precision		JDBC driver property: queryTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
resultsetMetaDataOptions	int		JDBC driver property: resultSetMetaDataOptions.
selectMethod	<ul style="list-style-type: none"> <li>• direct</li> <li>• cursor</li> </ul>		JDBC driver property: selectMethod.  <b>direct</b> direct <b>cursor</b> cursor
serverName	string	localhost	Server where the database is running.
snapshotSerializable	boolean		JDBC driver property: snapshotSerializable.

Attribute name	Data type	Default value	Description
spyAttributes	string		JDBC driver property: spyAttributes.
stringInputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringInputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
stringOutputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringOutputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
suppressConnectionWarnings	boolean		JDBC driver property: suppressConnectionWarnings.
transactionMode	<ul style="list-style-type: none"> <li>explicit</li> <li>implicit</li> </ul>		JDBC driver property: transactionMode. <b>explicit</b> explicit <b>implicit</b> implicit
truncateFractionalSeconds	boolean		JDBC driver property: truncateFractionalSeconds.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
useServerSideUpdatableCursors	boolean		JDBC driver property: useServerSideUpdatableCursors.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
validateServerCertificate	boolean		JDBC driver property: validateServerCertificate.

**oauthProvider > databaseStore > dataSource > properties.db2.i.native**

Data source properties for the IBM DB2 for i Native JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>read only</li> <li>all</li> <li>read call</li> </ul>	all	JDBC driver property: access. <b>read only</b> read only <b>all</b> all <b>read call</b> read call

Attribute name	Data type	Default value	Description
autoCommit	boolean	true	JDBC driver property: autoCommit.
batchStyle	<ul style="list-style-type: none"> <li>• 2.1</li> <li>• 2.0</li> </ul>	2.0	JDBC driver property: batchStyle. <b>2.1</b> 2.1 <b>2.0</b> 2.0
behaviorOverride	int		JDBC driver property: behaviorOverride.
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive
dataTruncation	string	true	JDBC driver property: dataTruncation.
databaseName	string	*LOCAL	JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy
dateSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		JDBC driver property: dateSeparator. <b>\,</b> The comma character (,). <b>b</b> The character b <b>.</b> The period character (.). <b>/</b> The forward slash character (/). <b>-</b> The dash character (-).
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		JDBC driver property: decimalSeparator. <b>\,</b> The comma character (,). <b>.</b> The period character (.).
directMap	boolean	true	JDBC driver property: directMap.
doEscapeProcessing	boolean	true	JDBC driver property: doEscapeProcessing.
fullErrors	boolean		JDBC driver property: fullErrors.
libraries	string		JDBC driver property: libraries.
lobThreshold	int Maximum: 500000	0	JDBC driver property: lobThreshold.

Attribute name	Data type	Default value	Description
lockTimeout	A period of time with second precision	0	JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>• 31</li> <li>• 63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 63
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
networkProtocol	int		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
prefetch	boolean	true	JDBC driver property: prefetch.
queryOptimizeGoal	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>	2	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).  <b>2</b> *ALLIO <b>1</b> *FIRSTIO

Attribute name	Data type	Default value	Description
reuseObjects	boolean	true	JDBC driver property: reuseObjects.
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
systemNaming	boolean	false	JDBC driver property: systemNaming.
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat.  <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  \, The comma character (,). <b>b</b> The character b : The colon character (:). . The period character (.).
trace	boolean		JDBC driver property: trace.
transactionTimeout	A period of time with second precision	0	JDBC driver property: transactionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateHex	<ul style="list-style-type: none"> <li>• binary</li> <li>• character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
useBlockInsert	boolean	false	JDBC driver property: useBlockInsert.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**oauthProvider > databaseStore > dataSource > properties.db2.i.toolbox**

Data source properties for the IBM DB2 for i Toolbox JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>• read only</li> <li>• all</li> <li>• read call</li> </ul>	all	JDBC driver property: access.  <b>read only</b> read only  <b>all</b> all  <b>read call</b> read call
behaviorOverride	int		JDBC driver property: behaviorOverride.
bidiImplicitReordering	boolean	true	JDBC driver property: bidiImplicitReordering.
bidiNumericOrdering	boolean	false	JDBC driver property: bidiNumericOrdering.
bidiStringType	int		JDBC driver property: bidiStringType.
bigDecimal	boolean	true	JDBC driver property: bigDecimal.
blockCriteria	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>	2	JDBC driver property: blockCriteria. Values are: 0 (no record blocking), 1 (block if FOR FETCH ONLY is specified), 2 (block if FOR UPDATE is specified).  <b>2</b> 2  <b>1</b> 1  <b>0</b> 0

Attribute name	Data type	Default value	Description
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> <li>• insensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive <b>insensitive</b> insensitive
dataCompression	boolean	true	JDBC driver property: dataCompression.
dataTruncation	boolean	true	JDBC driver property: dataTruncation.
databaseName	string		JDBC driver property: databaseName.
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy

Attribute name	Data type	Default value	Description
dateSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		<p>JDBC driver property: dateSeparator.</p> <p>The space character ( ).</p> <p>\, The comma character (,).</p> <p>. The period character (.).</p> <p>/ The forward slash character (/).</p> <p>- The dash character (-).</p>
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		<p>JDBC driver property: decimalSeparator.</p> <p>\, The comma character (,).</p> <p>. The period character (.).</p>
driver	<ul style="list-style-type: none"> <li>• toolbox</li> <li>• native</li> </ul>	toolbox	<p>JDBC driver property: driver.</p> <p><b>toolbox</b> toolbox</p> <p><b>native</b> native</p>
errors	<ul style="list-style-type: none"> <li>• full</li> <li>• basic</li> </ul>	basic	<p>JDBC driver property: errors.</p> <p><b>full</b> full</p> <p><b>basic</b> basic</p>
extendedDynamic	boolean	false	JDBC driver property: extendedDynamic.
extendedMetaData	boolean	false	JDBC driver property: extendedMetaData.
fullOpen	boolean	false	JDBC driver property: fullOpen.
holdInputLocators	boolean	true	JDBC driver property: holdInputLocators.
holdStatements	boolean	false	JDBC driver property: holdStatements.
isolationLevelSwitchingSupport	boolean	false	JDBC driver property: isolationLevelSwitchingSupport.
keepAlive	boolean		JDBC driver property: keepAlive.
lazyClose	boolean	false	JDBC driver property: lazyClose.
libraries	string		JDBC driver property: libraries.

Attribute name	Data type	Default value	Description
lobThreshold	int Minimum: 0 Maximum: 16777216	0	JDBC driver property: lobThreshold.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>• 31</li> <li>• 63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 64
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
metaDataSource	int Minimum: 0 Maximum: 1	1	JDBC driver property: metaDataSource.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
naming	<ul style="list-style-type: none"> <li>• system</li> <li>• sql</li> </ul>	sql	JDBC driver property: naming.  <b>system</b> system <b>sql</b> sql
package	string		JDBC driver property: package.
packageAdd	boolean	true	JDBC driver property: packageAdd.
packageCCSID	<ul style="list-style-type: none"> <li>• 13488</li> <li>• 1200</li> </ul>	13488	JDBC driver property: packageCCSID. Values are: 1200 (UCS-2) or 13488 (UTF-16).  <b>13488</b> 13488 (UTF-16) <b>1200</b> 1200 (UCS-2)
packageCache	boolean	false	JDBC driver property: packageCache.

Attribute name	Data type	Default value	Description
packageCriteria	<ul style="list-style-type: none"> <li>default</li> <li>select</li> </ul>	default	JDBC driver property: packageCriteria. <b>default</b> default <b>select</b> select
packageError	<ul style="list-style-type: none"> <li>exception</li> <li>none</li> <li>warning</li> </ul>	warning	JDBC driver property: packageError. <b>exception</b> exception <b>none</b> none <b>warning</b> warning
packageLibrary	string	QGPL	JDBC driver property: packageLibrary.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
prefetch	boolean	true	JDBC driver property: prefetch.
prompt	boolean	false	JDBC driver property: prompt.
proxyServer	string		JDBC driver property: proxyServer.
qaqqiniLibrary	string		JDBC driver property: qaqqiniLibrary.
queryOptimizeGoal	int Minimum: 0 Maximum: 2	0	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).
receiveBufferSize	int Minimum: 1		JDBC driver property: receiveBufferSize.
remarks	<ul style="list-style-type: none"> <li>system</li> <li>sql</li> </ul>	system	JDBC driver property: remarks. <b>system</b> system <b>sql</b> sql
rollbackCursorHold	boolean	false	JDBC driver property: rollbackCursorHold.
savePasswordWhenSerialized	boolean	false	JDBC driver property: savePasswordWhenSerialized.
secondaryUrl	string		JDBC driver property: secondaryUrl.
secure	boolean	false	JDBC driver property: secure.
sendBufferSize	int Minimum: 1		JDBC driver property: sendBufferSize.

Attribute name	Data type	Default value	Description
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
soLinger	A period of time with second precision		JDBC driver property: soLinger. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
soTimeout	A period of time with millisecond precision		JDBC driver property: soTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
sort	<ul style="list-style-type: none"> <li>• hex</li> <li>• table</li> <li>• language</li> </ul>	hex	JDBC driver property: sort. <b>hex</b> hex <b>table</b> table <b>language</b> language
sortLanguage	string		JDBC driver property: sortLanguage.
sortTable	string		JDBC driver property: sortTable.
sortWeight	<ul style="list-style-type: none"> <li>• unqiue</li> <li>• shared</li> </ul>		JDBC driver property: sortWeight. <b>unqiue</b> unique <b>shared</b> shared
tcpNoDelay	boolean		JDBC driver property: tcpNoDelay.
threadUsed	boolean	true	JDBC driver property: threadUsed.

Attribute name	Data type	Default value	Description
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat. <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  The space character ( ). \, The comma character (,). : The colon character (:). . The period character (.).
toolboxTrace	<ul style="list-style-type: none"> <li>• diagnostic</li> <li>• information</li> <li>• conversion</li> <li>• error</li> <li>• thread</li> <li>• proxy</li> <li>• none</li> <li>• datastream</li> <li>• pcml</li> <li>• all</li> <li>• jdbc</li> <li>• warning</li> </ul>		JDBC driver property: toolboxTrace. <b>diagnostic</b> diagnostic <b>information</b> information <b>conversion</b> conversion <b>error</b> error <b>thread</b> thread <b>proxy</b> proxy <b>none</b> none <b>datastream</b> datastream <b>pcml</b> pcml <b>all</b> all <b>jdbc</b> jdbc <b>warning</b> warning
trace	boolean		JDBC driver property: trace.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateBoolean	boolean	true	JDBC driver property: translateBoolean.

Attribute name	Data type	Default value	Description
translateHex	<ul style="list-style-type: none"> <li>binary</li> <li>character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
trueAutoCommit	boolean	false	JDBC driver property: trueAutoCommit.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaLooselyCoupledSupport	int  Minimum: 0  Maximum: 1	0	JDBC driver property: xaLooselyCoupledSupport.

**oauthProvider > databaseStore > dataSource > properties.db2.jcc**

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for DB2.

false

Attribute name	Data type	Default value	Description
activateDatabase	int		JDBC driver property: activateDatabase.
alternateGroupDatabaseName	string		JDBC driver property: alternateGroupDatabaseName.
alternateGroupPortNumber	string		JDBC driver property: alternateGroupPortNumber.
alternateGroupServerName	string		JDBC driver property: alternateGroupServerName.
blockingReadConnectionTimeout	A period of time with second precision		JDBC driver property: blockingReadConnectionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
clientAccountingInformation	string		JDBC driver property: clientAccountingInformation.
clientApplicationInformation	string		JDBC driver property: clientApplicationInformation.
clientRerouteAlternatePortNumber	string		JDBC driver property: clientRerouteAlternatePortNumber.
clientRerouteAlternateServerName	string		JDBC driver property: clientRerouteAlternateServerName.

Attribute name	Data type	Default value	Description
clientUser	string		JDBC driver property: clientUser.
clientWorkstation	string		JDBC driver property: clientWorkstation.
connectionCloseWithInFlightTransaction	Transaction • 1		JDBC driver property: connectionCloseWithInFlightTransaction. 2 CONNECTION_CLOSE_WITH_ROLLBACK 1 CONNECTION_CLOSE_WITH_EXCEPTION
currentAlternateGroupEntry	int		JDBC driver property: currentAlternateGroupEntry.
currentFunctionPath	string		JDBC driver property: currentFunctionPath.
currentLocaleLcCtype	string		JDBC driver property: currentLocaleLcCtype.
currentLockTimeout	A period of time with second precision		JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
currentPackagePath	string		JDBC driver property: currentPackagePath.
currentPackageSet	string		JDBC driver property: currentPackageSet.
currentSQLID	string		JDBC driver property: currentSQLID.
currentSchema	string		JDBC driver property: currentSchema.
cursorSensitivity	• 2 • 1 • 0		JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). 2 TYPE_SCROLL_ASENSITIVE 1 TYPE_SCROLL_SENSITIVE_DYNAMIC 0 TYPE_SCROLL_SENSITIVE_STATIC
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean	true	JDBC driver property: deferPrepares.

Attribute name	Data type	Default value	Description
driverType	<ul style="list-style-type: none"> <li>2</li> <li>4</li> </ul>	4	JDBC driver property: driverType. 2 Type 2 JDBC driver. 4 Type 4 JDBC driver.
enableAlternateGroupSeamlessACR	boolean		JDBC driver property: enableAlternateGroupSeamlessACR.
enableClientAffinitiesList	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableClientAffinitiesList. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableExtendedDescribe	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedDescribe. 2 NO 1 YES
enableExtendedIndicators	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedIndicators. 2 NO 1 YES
enableNamedParameterMarkers	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSeamlessFailover	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeInputStreams	boolean		JDBC driver property: fullyMaterializeInputStreams.
fullyMaterializeInputStreamsOnBatchExecution	<ul style="list-style-type: none"> <li>1</li> </ul>		JDBC driver property: fullyMaterializeInputStreamsOnBatchExecution. 2 NO 1 YES
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.

Attribute name	Data type	Default value	Description
implicitRollbackOption	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: implicitRollbackOption.</p> <p>2 IMPLICIT_ROLLBACK_OPTION_CLOSE</p> <p>1 IMPLICIT_ROLLBACK_OPTION_NO</p> <p>0 IMPLICIT_ROLLBACK_OPTION_NO</p>
interruptProcessingMode	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: interruptProcessingMode.</p> <p>2 INTERRUPT_PROCESSING_MODE_C</p> <p>1 INTERRUPT_PROCESSING_MODE_S</p> <p>0 INTERRUPT_PROCESSING_MODE_D</p>
keepAliveTimeOut	A period of time with second precision		<p>JDBC driver property: keepAliveTimeOut. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
keepDynamic	int		JDBC driver property: keepDynamic.
kerberosServerPrincipal	string		JDBC driver property: kerberosServerPrincipal.
loginTimeout	A period of time with second precision		<p>JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
maxConnCachedParamBufferSize	int		JDBC driver property: maxConnCachedParamBufferSize.
maxRetriesForClientReroute	int		JDBC driver property: maxRetriesForClientReroute.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	50000	Port on which to obtain database connections.
profileName	string		JDBC driver property: profileName.

Attribute name	Data type	Default value	Description
queryCloseImplicit	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: queryCloseImplicit. Values are: 1 (QUERY_CLOSE_IMPLICIT_YES) or 2 (QUERY_CLOSE_IMPLICIT_NO).</p> <p>2        QUERY_CLOSE_IMPLICIT_NO 1        QUERY_CLOSE_IMPLICIT_YES</p>
queryDataSize	<p>int</p> <p>Minimum: 4096</p> <p>Maximum: 65535</p>		JDBC driver property: queryDataSize.
queryTimeoutInterruptProcessingMode	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: queryTimeoutInterruptProcessingMode.</p> <p>2        INTERRUPT_PROCESSING_MODAL 1        INTERRUPT_PROCESSING_MODAL</p>
readOnly	boolean		JDBC driver property: readOnly.
recordTemporalHistory	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: recordTemporalHistory.</p> <p>2        NO 1        YES</p>
resultSetHoldability	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2        CLOSE_CURSORS_AT_COMMIT 1        HOLD_CURSORS_OVER_COMMIT</p>
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2        CLOSE_CURSORS_AT_COMMIT 1        HOLD_CURSORS_OVER_COMMIT</p>
retrieveMessagesFromServerOnGetMessage	boolean	true	JDBC driver property: retrieveMessagesFromServerOnGetMessage.

Attribute name	Data type	Default value	Description
retryIntervalForClientReroute	A period of time with second precision		JDBC driver property: retryIntervalForClientReroute. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 18</li> <li>• 15</li> <li>• 9</li> <li>• 16</li> <li>• 13</li> <li>• 11</li> <li>• 12</li> </ul>		<p>JDBC driver property: securityMechanism. Values are:</p> <ul style="list-style-type: none"> <li>3 (CLEAR_TEXT_PASSWORD_SECURITY),</li> <li>4 (USER_ONLY_SECURITY),</li> <li>7 (ENCRYPTED_PASSWORD_SECURITY),</li> <li>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY),</li> <li>11 (KERBEROS_SECURITY),</li> <li>12 (ENCRYPTED_USER_AND_DATA_SECURITY),</li> <li>13 (ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY),</li> <li>15 (PLUGIN_SECURITY),</li> <li>16 (ENCRYPTED_USER_ONLY_SECURITY),</li> <li>18 (TLS_CLIENT_CERTIFICATE_SECURITY).</li> </ul> <p>3 CLEAR_TEXT_PASSWORD_SECURITY  7 ENCRYPTED_PASSWORD_SECURITY  4 USER_ONLY_SECURITY  18 TLS_CLIENT_CERTIFICATE_SECURITY  15 PLUGIN_SECURITY  9 ENCRYPTED_USER_AND_PASSWORD_SECURITY  16 ENCRYPTED_USER_ONLY_SECURITY  13 ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY  11 KERBEROS_SECURITY  12 ENCRYPTED_USER_AND_DATA_SECURITY</p>
sendDataAsIs	boolean		JDBC driver property: sendDataAsIs.
serverName	string	localhost	Server where the database is running.
sessionTimeZone	string		JDBC driver property: sessionTimeZone.
sqljCloseStmtsWithOpenResultSet	boolean		JDBC driver property: sqljCloseStmtsWithOpenResultSet.

Attribute name	Data type	Default value	Description
sqljEnableClassLoaderSpecificProfiles	boolean		JDBC driver property: sqljEnableClassLoaderSpecificProfiles.
sslConnection	boolean		JDBC driver property: sslConnection.
streamBufferSize	int		JDBC driver property: streamBufferSize.
stripTrailingZerosForDecimalNumbers	Numbers <ul style="list-style-type: none"> <li>• 1</li> </ul>		JDBC driver property: stripTrailingZerosForDecimalNumbers. 2 NO 1 YES
sysSchema	string		JDBC driver property: sysSchema.
timerLevelForQueryTimeOut	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• -1</li> </ul>		JDBC driver property: timerLevelForQueryTimeOut. 2 QUERYTIMEOUT_CONNECTION 1 QUERYTIMEOUT_STATEMENT_L -1 QUERYTIMEOUT_DISABLED
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceFileCount	int		JDBC driver property: traceFileCount.
traceFileSize	int		JDBC driver property: traceFileSize.
traceLevel	int	0	Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
traceOption	<ul style="list-style-type: none"> <li>• 1</li> <li>• 0</li> </ul>		JDBC driver property: traceOption 1 1 0 0

Attribute name	Data type	Default value	Description
translateForBitData	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: translateForBitData. 2 SERVER_ENCODING_REPRESENTATION 1 HEX_REPRESENTATION
updateCountForBatch	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: updateCountForBatch. 2 TOTAL_UPDATE_COUNT 1 NO_UPDATE_COUNT
useCachedCursor	boolean		JDBC driver property: useCachedCursor.
useIdentityValLocalForAutoGeneratedKeys	boolean		JDBC driver property: useIdentityValLocalForAutoGeneratedKeys.
useJDBC41DefinitionForGetColumns	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC41DefinitionForGetColumns. 2 NO 1 YES
useJDBC4ColumnNameAndLabelSemantics	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
useTransactionRedirect	boolean		JDBC driver property: useTransactionRedirect.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaNetworkOptimization	boolean		JDBC driver property: xaNetworkOptimization.

**oauthProvider > databaseStore > dataSource > properties.derby.client**

Data source properties for Derby Network Client JDBC driver.

false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1527	Port on which to obtain database connections.
retrieveMessageText	boolean	true	JDBC driver property: retrieveMessageText.
securityMechanism	<ul style="list-style-type: none"> <li>3</li> <li>7</li> <li>4</li> <li>9</li> <li>8</li> </ul>	3	<p>JDBC driver property: securityMechanism. Values are:</p> <p>3 (CLEAR_TEXT_PASSWORD_SECURITY),</p> <p>4 (USER_ONLY_SECURITY),</p> <p>7 (ENCRYPTED_PASSWORD_SECURITY),</p> <p>8 (STRONG_PASSWORD_SUBSTITUTE_SECURITY),</p> <p>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY)</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY</p> <p>7 ENCRYPTED_PASSWORD_SECURITY</p> <p>4 USER_ONLY_SECURITY</p> <p>9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p> <p>8 STRONG_PASSWORD_SUBSTITUTE_SECURITY</p>

Attribute name	Data type	Default value	Description
serverName	string	localhost	Server where the database is running.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		JDBC driver property: shutdownDatabase. <b>false</b> Do not shut down the database. <b>shutdown</b> Shut down the database when a connection is attempted.
ssl	<ul style="list-style-type: none"> <li>basic</li> <li>off</li> <li>peerAuthentication</li> </ul>		JDBC driver property: ssl. <b>basic</b> basic <b>off</b> off <b>peerAuthentication</b> peerAuthentication
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_XA_CALLS=2048, TRACE_ALL=-1.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**oauthProvider > databaseStore > dataSource > properties.derby.embedded**

Data source properties for Derby Embedded JDBC driver.

false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		<p>JDBC driver property: shutdownDatabase.</p> <p><b>false</b> Do not shut down the database.</p> <p><b>shutdown</b> Shut down the database when a connection is attempted.</p>
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**oauthProvider > databaseStore > dataSource > properties.informix**

Data source properties for the Informix JDBC driver.

false

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
ifxCLIENT_LOCALE	string		JDBC driver property: ifxCLIENT_LOCALE.
ifxCPMAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMInitPoolSize	int		JDBC driver property: ifxCPMInitPoolSize.
ifxCPMMaxConnections	int		JDBC driver property: ifxCPMMaxConnections.
ifxCPMMaxPoolSize	int		JDBC driver property: ifxCPMMaxPoolSize.
ifxCPMMinAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMMinAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMMinPoolSize	int		JDBC driver property: ifxCPMMinPoolSize.
ifxCPMServiceInterval	A period of time with millisecond precision		JDBC driver property: ifxCPMServiceInterval. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxDBANSIWARN	boolean		JDBC driver property: ifxDBANSIWARN.
ifxDBCENTURY	string		JDBC driver property: ifxDBCENTURY.
ifxDBDATE	string		JDBC driver property: ifxDBDATE.
ifxDBSPACETEMP	string		JDBC driver property: ifxDBSPACETEMP.

Attribute name	Data type	Default value	Description
ifxDBTEMP	string		JDBC driver property: ifxDBTEMP.
ifxDBTIME	string		JDBC driver property: ifxDBTIME.
ifxDBUPSPACE	string		JDBC driver property: ifxDBUPSPACE.
ifxDB_LOCALE	string		JDBC driver property: ifxDB_LOCALE.
ifxDELIMIDENT	boolean		JDBC driver property: ifxDELIMIDENT.
ifxENABLE_TYPE_CACHE	boolean		JDBC driver property: ifxENABLE_TYPE_CACHE.
ifxFET_BUF_SIZE	int		JDBC driver property: ifxFET_BUF_SIZE.
ifxGL_DATE	string		JDBC driver property: ifxGL_DATE.
ifxGL_DATETIME	string		JDBC driver property: ifxGL_DATETIME.
ifxIFXHOST	string	localhost	JDBC driver property: ifxIFXHOST.
ifxIFX_AUTOFREE	boolean		JDBC driver property: ifxIFX_AUTOFREE.
ifxIFX_DIRECTIVES	string		JDBC driver property: ifxIFX_DIRECTIVES.
ifxIFX_LOCK_MODE_WAIT	A period of time with second precision	2s	JDBC driver property: ifxIFX_LOCK_MODE_WAIT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxIFX_SOC_TIMEOUT	A period of time with millisecond precision		JDBC driver property: ifxIFX_SOC_TIMEOUT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxIFX_USEPUT	boolean		JDBC driver property: ifxIFX_USEPUT.

Attribute name	Data type	Default value	Description
ifxIFX_USE_STRENC	boolean		JDBC driver property: ifxIFX_USE_STRENC.
ifxIFX_XASPEC	string	y	JDBC driver property: ifxIFX_XASPEC.
ifxINFORMIXCONRETRY	int		JDBC driver property: ifxINFORMIXCONRETRY.
ifxINFORMIXCONTIME	A period of time with second precision		JDBC driver property: ifxINFORMIXCONTIME. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxINFORMIXOPCACHE	string		JDBC driver property: ifxINFORMIXOPCACHE.
ifxINFORMIXSTACKSIZE	int		JDBC driver property: ifxINFORMIXSTACKSIZE.
ifxJDBCTEMP	string		JDBC driver property: ifxJDBCTEMP.
ifxLDAP_IFXBASE	string		JDBC driver property: ifxLDAP_IFXBASE.
ifxLDAP_PASSWD	string		JDBC driver property: ifxLDAP_PASSWD.
ifxLDAP_URL	string		JDBC driver property: ifxLDAP_URL.
ifxLDAP_USER	string		JDBC driver property: ifxLDAP_USER.
ifxLOBCACHE	int		JDBC driver property: ifxLOBCACHE.
ifxNEWCODESET	string		JDBC driver property: ifxNEWCODESET.
ifxNEWLOCALE	string		JDBC driver property: ifxNEWLOCALE.
ifxNODEFDAC	string		JDBC driver property: ifxNODEFDAC.
ifxOPTCOMPIND	string		JDBC driver property: ifxOPTCOMPIND.
ifxOPTOFC	string		JDBC driver property: ifxOPTOFC.
ifxOPT_GOAL	string		JDBC driver property: ifxOPT_GOAL.
ifxPATH	string		JDBC driver property: ifxPATH.
ifxPDQPRIORITY	string		JDBC driver property: ifxPDQPRIORITY.

Attribute name	Data type	Default value	Description
ifxPLCONFIG	string		JDBC driver property: ifxPLCONFIG.
ifxPLOAD_LO_PATH	string		JDBC driver property: ifxPLOAD_LO_PATH.
ifxPROTOCOLTRACE	int		JDBC driver property: ifxPROTOCOLTRACE.
ifxPROTOCOLTRACEFILE	string		JDBC driver property: ifxPROTOCOLTRACEFILE.
ifxPROXY	string		JDBC driver property: ifxPROXY.
ifxPSORT_DBTEMP	string		JDBC driver property: ifxPSORT_DBTEMP.
ifxPSORT_NPROCS	boolean		JDBC driver property: ifxPSORT_NPROCS.
ifxSECURITY	string		JDBC driver property: ifxSECURITY.
ifxSQLH_FILE	string		JDBC driver property: ifxSQLH_FILE.
ifxSQLH_LOC	string		JDBC driver property: ifxSQLH_LOC.
ifxSQLH_TYPE	string		JDBC driver property: ifxSQLH_TYPE.
ifxSSLCONNECTION	string		JDBC driver property: ifxSSLCONNECTION.
ifxSTMT_CACHE	string		JDBC driver property: ifxSTMT_CACHE.
ifxTRACE	int		JDBC driver property: ifxTRACE.
ifxTRACEFILE	string		JDBC driver property: ifxTRACEFILE.
ifxTRUSTED_CONTEXT	string		JDBC driver property: ifxTRUSTED_CONTEXT.
ifxUSEV5SERVER	boolean		JDBC driver property: ifxUSEV5SERVER.
ifxUSE_DTENV	boolean		JDBC driver property: ifxUSE_DTENV.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
roleName	string		JDBC driver property: roleName.
serverName	string		Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**oauthProvider > databaseStore > dataSource > properties.informix.jcc**

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for Informix.  
false

Attribute name	Data type	Default value	Description
DBANSIWARN	boolean		JDBC driver property: DBANSIWARN.
DBDATE	string		JDBC driver property: DBDATE.
DBPATH	string		JDBC driver property: DBPATH.
DBSPACETEMP	string		JDBC driver property: DBSPACETEMP.
DBTEMP	string		JDBC driver property: DBTEMP.
DBUPSPACE	string		JDBC driver property: DBUPSPACE.
DELIMIDENT	boolean		JDBC driver property: DELIMIDENT.
IFX_DIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_DIRECTIVES. <b>ON</b> ON <b>OFF</b> OFF
IFX_EXTDIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_EXTDIRECTIVES. <b>ON</b> ON <b>OFF</b> OFF
IFX_UPDESC	string		JDBC driver property: IFX_UPDESC.

Attribute name	Data type	Default value	Description
IFX_XASTDCOMPLIANCE_XAEND	<ul style="list-style-type: none"> <li>0</li> </ul>		JDBC driver property: IFX_XASTDCOMPLIANCE_XAEND. <b>1</b> 1 <b>0</b> 0
INFORMIXOPCACHE	string		JDBC driver property: INFORMIXOPCACHE.
INFORMIXSTACKSIZE	string		JDBC driver property: INFORMIXSTACKSIZE.
NODEFDAC	<ul style="list-style-type: none"> <li>yes</li> <li>no</li> </ul>		JDBC driver property: NODEFDAC. <b>yes</b> yes <b>no</b> no
OPTCOMPIND	<ul style="list-style-type: none"> <li>2</li> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTCOMPIND. <b>2</b> 2 <b>1</b> 1 <b>0</b> 0
OPTOFC	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTOFC. <b>1</b> 1 <b>0</b> 0
PDQPRIORITY	<ul style="list-style-type: none"> <li>HIGH</li> <li>LOW</li> <li>OFF</li> </ul>		JDBC driver property: PDQPRIORITY. <b>HIGH</b> HIGH <b>LOW</b> LOW <b>OFF</b> OFF
PSORT_DBTEMP	string		JDBC driver property: PSORT_DBTEMP.
PSORT_NPROCS	string Maximum: 10		JDBC driver property: PSORT_NPROCS.
STMT_CACHE	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: STMT_CACHE. <b>1</b> 1 <b>0</b> 0
currentLockTimeout	A period of time with second precision	2s	JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean		JDBC driver property: deferPrepares.
driverType	int	4	JDBC driver property: driverType.
enableNamedParameterMarkers	int		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO).
enableSeamlessFailover	int		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO).
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.
keepDynamic	int		JDBC driver property: keepDynamic.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
progressiveStreaming	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		JDBC driver property: progressiveStreaming. Values are: 1 (YES) or 2 (NO).  2      NO 1      YES
queryDataSize	int  Minimum: 4096  Maximum: 10485760		JDBC driver property: queryDataSize.

Attribute name	Data type	Default value	Description
resultSetHoldability	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
retrieveMessagesFromServerOnGetMessage	boolean	true	<p>JDBC driver property: retrieveMessagesFromServerOnGetMessage.</p>
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 9</li> </ul>		<p>JDBC driver property: securityMechanism. Values are: 3 (CLEAR_TEXT_PASSWORD_SECURITY), 4 (USER_ONLY_SECURITY), 7 (ENCRYPTED_PASSWORD_SECURITY), 9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY).</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY 7 ENCRYPTED_PASSWORD_SECURITY 4 USER_ONLY_SECURITY 9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p>
serverName	string	localhost	Server where the database is running.
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.

Attribute name	Data type	Default value	Description
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
useJDBC4ColumnNameAndLabelSemantics	boolean		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO).
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**oauthProvider > databaseStore > dataSource > properties.microsoft.sqlserver**

Data source properties for Microsoft SQL Server JDBC Driver.

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database. Example: jdbc:sqlserver://localhost:1433;databaseName=myDB.
applicationIntent	<ul style="list-style-type: none"> <li>ReadOnly</li> <li>ReadWrite</li> </ul>		JDBC driver property: applicationIntent. <b>ReadOnly</b> ReadOnly <b>ReadWrite</b> ReadWrite
applicationName	string		JDBC driver property: applicationName.
authenticationScheme	<ul style="list-style-type: none"> <li>NativeAuthentication</li> <li>JavaKerberos</li> </ul>		JDBC driver property: authenticationScheme. <b>NativeAuthentication</b> NativeAuthentication <b>JavaKerberos</b> JavaKerberos

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
encrypt	boolean		JDBC driver property: encrypt.
failoverPartner	string		JDBC driver property: failoverPartner.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
instanceName	string		JDBC driver property: instanceName.
integratedSecurity	boolean		JDBC driver property: integratedSecurity.
lastUpdateCount	boolean		JDBC driver property: lastUpdateCount.
lockTimeout	A period of time with millisecond precision		JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
multiSubnetFailover	boolean		JDBC driver property: multiSubnetFailover.
packetSize	int Minimum: 512 Maximum: 32767		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.

Attribute name	Data type	Default value	Description
responseBuffering	<ul style="list-style-type: none"> <li>full</li> <li>adaptive</li> </ul>		JDBC driver property: responseBuffering. <b>full</b> full <b>adaptive</b> adaptive
selectMethod	<ul style="list-style-type: none"> <li>direct</li> <li>cursor</li> </ul>		JDBC driver property: selectMethod. <b>direct</b> direct <b>cursor</b> cursor
sendStringParametersAsUnicode	boolean	false	JDBC driver property: sendStringParametersAsUnicode.
sendTimeAsDatetime	boolean		JDBC driver property: sendTimeAsDatetime.
serverName	string	localhost	Server where the database is running.
trustServerCertificate	boolean		JDBC driver property: trustServerCertificate.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
workstationID	string		JDBC driver property: workstationID.
xopenStates	boolean		JDBC driver property: xopenStates.

**oauthProvider > databaseStore > dataSource > properties.oracle**

Data source properties for Oracle JDBC driver.

false

Attribute name	Data type	Default value	Description
ONSConfiguration	string		JDBC driver property: ONSConfiguration.
TNSEntryName	string		JDBC driver property: TNSEntryName.
URL	string		URL for connecting to the database. Examples: jdbc:oracle:thin://localhost:1521/sample or jdbc:oracle:oci://localhost:1521/sample.
connectionProperties	string		JDBC driver property: connectionProperties.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
driverType	<ul style="list-style-type: none"> <li>oci</li> <li>thin</li> </ul>	thin	JDBC driver property: driverType.  <b>oci</b> oci <b>thin</b> thin
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	string		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1521	Port on which to obtain database connections.
serverName	string	localhost	Server where the database is running.
serviceName	string		JDBC driver property: serviceName.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**oauthProvider > databaseStore > dataSource > properties.sybase**

Data source properties for Sybase JDBC driver.

false

Attribute name	Data type	Default value	Description
SERVER_INITIATED_TRANSACTIONS	<ul style="list-style-type: none"> <li>false</li> <li>true</li> </ul>	false	JDBC driver property: SERVER_INITIATED_TRANSACTIONS.  <b>false</b> false <b>true</b> true
connectionProperties	string	SELECT_OPENS_CURSOR=true	JDBC driver property: connectionProperties.
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	<ul style="list-style-type: none"> <li>• SSL</li> <li>• socket</li> </ul>		JDBC driver property: networkProtocol.  <b>SSL</b> SSL <b>socket</b> socket
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	5000	Port on which to obtain database connections.
resourceManagerName	string		JDBC driver property: resourceManagerName.
serverName	string	localhost	Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
version	int		JDBC driver property: version.

**oauthProvider > databaseStore > dataSource > recoveryAuthData**

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

**oauthProvider > grantType**

An access token grant type (as detailed in the OAuth specification) that is allowed for the provider. The equivalent provider parameter in the full application server profile is `oauth20.grant.types.allowed`.

false

string

**oauthProvider > jwtGrantType**

The `grant_type` for JWT Token handler

false

Attribute name	Data type	Default value	Description
clockSkew	A period of time with second precision	300s	The time difference allowed between OpenID Connect Client and OpenID Connect Provider systems when they are not synchronized. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
iatRequired	boolean	false	The iat claim in a jwt token is required.
maxJtiCacheSize	long Minimum: 1	10000	The maximum size of cache, which keeps jti data of jwt token, to prevent the jti from being reused.
tokenMaxLifetime	A period of time with second precision	7200s	The time indicates the maximum lifetime of an alive jwt token since its issued-at-time. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**oauthProvider > library**

Reference to shared library containing the mediator plugin class.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

**oauthProvider > library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**oauthProvider > library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**oauthProvider > library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**oauthProvider > localStore**

Clients are defined in server.xml and tokens are cached in the server.

false

Attribute name	Data type	Default value	Description
tokenStoreSize	long	2000	Token store size

**oauthProvider > localStore > client**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
applicationType	<ul style="list-style-type: none"> <li>• native</li> <li>• web</li> </ul>	web	The type of application best describing the client. <b>native</b> native <b>web</b> web
displayname	string		Display name of the client.
enabled	boolean	true	Client is enabled if true, disabled if false.

Attribute name	Data type	Default value	Description
functionalUserId	string		A user identifier to be associated with access tokens obtained by this client using the client credentials grant type. When this client parameter is specified, the value is returned in the functional_user_id response parameter from the introspect endpoint.
id	string		A unique configuration ID.
introspectTokens	boolean	false	Boolean value specifying whether the client is allowed to access the introspection endpoint to introspect tokens issued by the authorization server.
name	string		Name of the client (sometimes referred to as the Id).
preAuthorizedScope	string		Space separated list of scope values that the client can use when requesting access tokens that are deemed to have been pre-approved by the resource owner and therefore does not require the resource owner's consent.
scope	string		Specify by spaces the list of scopes of the client.
secret	Reversably encoded password (string)		Secret key of the client.
sessionManaged	boolean	false	Boolean indicating whether the client participates in OpenID session management.
subjectType	<ul style="list-style-type: none"> <li>public</li> </ul>		Subject type requested for response to this client. <b>public</b> public
tokenEndpointAuthMethod	<ul style="list-style-type: none"> <li>client_secret_post</li> <li>none</li> <li>client_secret_basic</li> </ul>	client_secret_basic	The requested authentication method for the token endpoint of the client. <b>client_secret_post</b> client_secret_post <b>none</b> none <b>client_secret_basic</b> client_secret_basic

**oauthProvider > localStore > client > functionalUserGroupIds**

A list of group ids to be associated with access tokens obtained by this client using the client credentials grant type. When this client parameter is specified, the value is returned in the functional\_user\_groupIds response parameter from the introspect endpoint.

false

string

**oauthProvider > localStore > client > grantTypes**

Grant types the client may use.

false

**oauthProvider > localStore > client > postLogoutRedirectUris**

Array of URLs supplied by the RP to which it may request that the end-user's user agent be redirected using the post\_logout\_redirect\_uri parameter after a logout has been performed.

false

string

**oauthProvider > localStore > client > redirect**

Array of redirect URIs for use in redirect-based flows such as the authorization code and implicit grant types of the client. The first redirect URI is used as a default, when none is specified in a request.

false

string

**oauthProvider > localStore > client > responseTypes**

Response types the client may use.

false

**oauthProvider > mediatorClassName**

Mediator plugin class name. The equivalent provider parameter in the full application server profile is oauth20.mediator.classnames.

false

string

**scopeToClaimMap**

Specify the claims for the scope.

false

Attribute name	Data type	Default value	Description
address	string	address	Specify a comma-separated list of claims associated with the address scope.
email	string	email, email_verified	Specify a comma-separated list of claims associated with the email scope.
phone	string	phone_number, phone_number_verified	Specify a comma-separated list of claims associated with the phone scope.

Attribute name	Data type	Default value	Description
profile	string	name, family_name, given_name, middle_name, nickname, preferred_username, profile, picture, website, gender, birthdate, zoneinfo, locale, updated_at	Specify a comma-separated list of claims associated with the profile scope.

**scopeToClaimMap > property**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Specify the name of the property
value	string		Specify the value of the property

## Object Request Broker (ORB) (orb)

Configuration for a server or client ORB. Specify either the nameService attribute for a client ORB or one or more iiopEndpoint references for a server ORB.

- clientPolicy.clientContainerCsiv2
  - layers
    - authenticationLayer
      - mechanisms
    - transportLayer
- clientPolicy.csiv2
  - layers
    - attributeLayer
      - identityAssertionTypes
    - authenticationLayer
      - mechanisms
    - transportLayer
- iiopEndpoint
  - iiopsOptions
  - tcpOptions
- serverPolicy.csiv2
  - layers
    - attributeLayer
      - identityAssertionTypes
    - authenticationLayer
      - mechanisms
    - transportLayer

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
iiopEndpointRef	List of references to top level iiopEndpoint elements (comma-separated string).	defaultIiopEndpoint	Optional IIOP Endpoint describing the ports open for this ORB
nameService	string	corbaname::localhost:2809	Optional URL for the remote name service, for example corbaname::localhost:2809

### **clientPolicy.clientContainerCsiV2**

Common Secure Interoperability Version 2 (CSIv2) for outgoing Internet Inter-ORB Protocol (IIOP) requests.

false

#### **clientPolicy.clientContainerCsiV2 > layers**

Specify the CSIv2 layers like transport, authentication, and attribute.

false

#### **clientPolicy.clientContainerCsiV2 > layers > authenticationLayer**

Determine the authentication mechanisms and association options to be performed by the client for outgoing CSIv2 requests.

false

Attribute name	Data type	Default value	Description
establishTrustInClient	<ul style="list-style-type: none"> <li>• Required</li> <li>• Never</li> <li>• Supported</li> </ul>	Supported	<p>Specify if this association option is Supported, Required, or Never used for this layer. It indicates the authentication requirements at the authentication layer.</p> <p><b>Required</b> The association option is required</p> <p><b>Never</b> The association option must not be used</p> <p><b>Supported</b> The association option is supported</p>
password	Reversably encoded password (string)		The user password that is used with the user name.
user	string		The user name that is used to login to the remote server.

#### **clientPolicy.clientContainerCsiV2 > layers > authenticationLayer > mechanisms**

Specifies authentication mechanisms as a comma separated list. For example: GSSUP

false

string

**clientPolicy.clientContainerCsiv2 > layers > transportLayer**

Configure how to trust the client.

false

Attribute name	Data type	Default value	Description
sslEnabled	boolean	true	Indicate by true or false whether SSL is enabled for CSiv2 requests. Default is true and is the recommended value. If this attribute is set to false, sensitive information such as passwords and tokens are sent over unsecured channels when using IIOP.
sslRef	A reference to top level ssl element (string).		Specify the SSL configuration needed to establish a secure connection.

**clientPolicy.csiv2**

Common Secure Interoperability Version 2 (CSiv2) for outgoing Internet Inter-ORB Protocol (IIOP) requests.

false

**clientPolicy.csiv2 > layers**

Specify the CSiv2 layers like transport, authentication, and attribute.

false

**clientPolicy.csiv2 > layers > attributeLayer**

Determine the attribute layer options to be performed by the client for outgoing CSiv2 requests.

false

Attribute name	Data type	Default value	Description
identityAssertionEnabled	boolean	false	Indicate by true or false whether identity assertion is enabled. Default is false.
trustedIdentity	string		The trusted identity used to assert an entity to the remote server.
trustedPassword	Reversably encoded password (string)		Specify the password that is used with the trusted identity.

**clientPolicy.csiv2 > layers > attributeLayer > identityAssertionTypes**

Specify the supported identity token types for identity assertion.

false

**clientPolicy.csiv2 > layers > authenticationLayer**

Determine the authentication mechanisms and association options to be performed by the client for outgoing CSiv2 requests.

false

Attribute name	Data type	Default value	Description
establishTrustInClient	<ul style="list-style-type: none"> <li>Required</li> <li>Never</li> <li>Supported</li> </ul>	Supported	<p>Specify if this association option is Supported, Required, or Never used for this layer. It indicates authentication requirements at the authentication layer.</p> <p><b>Required</b> The association option is required</p> <p><b>Never</b> The association option must not be used</p> <p><b>Supported</b> The association option is supported</p>

**clientPolicy.csiv2 > layers > authenticationLayer > mechanisms**

Specifies authentication mechanisms as a comma separated list. For example: GSSUP, LTPA

false

string

**clientPolicy.csiv2 > layers > transportLayer**

Configure how to trust the client.

false

Attribute name	Data type	Default value	Description
sslEnabled	boolean	true	Indicate by true or false whether SSL is enabled for CSiv2 requests. Default is true and is the recommended value. If this attribute is set to false, sensitive information such as passwords and tokens are sent over unsecured channels when using IIOp.
sslRef	A reference to top level ssl element (string).		Specify the SSL configuration needed to establish a secure connection.

**iioEndpoint**

Optional IIOp Endpoint describing the ports open for this ORB

false

Attribute name	Data type	Default value	Description
host	string	localhost	IP address, domain name server (DNS) host name with domain name suffix, or just the DNS host name

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
iiopPort	int		Port for the unsecured server socket opened by this IIOP endpoint
tcpOptionsRef	A reference to top level tcpOptions element (string).	defaultTCPOptions	TCP protocol options for the IIOP endpoint

### **iiopEndpoint > iiopsOptions**

Specification of a secured server socket opened by this IIOP endpoint

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
iiopsPort	int		Specify the port to be configured with the SSL options.
sessionTimeout	A period of time with second precision	1d	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
sslRef	A reference to top level ssl element (string).		The default SSL configuration repertoire. The default value is defaultSSLSettings.
suppressHandshakeErrors	boolean	false	Disable logging of SSL handshake errors. SSL handshake errors can occur during normal operation, however these messages can be useful when SSL is behaving unexpectedly.

### **iiopEndpoint > tcpOptions**

TCP protocol options for the IIOP endpoint

false

Attribute name	Data type	Default value	Description
inactivityTimeout	A period of time with millisecond precision	60s	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
soReuseAddr	boolean	true	Enables immediate rebind to a port with no active listener.

### **serverPolicy.csiv2**

Common Secure Interoperability Version 2 (CSIV2) for incoming Internet Inter-ORB Protocol (IIOP) requests.

false

#### **serverPolicy.csiv2 > layers**

Specify the CSIV2 layers like transport, authentication, and attribute.

false

#### **serverPolicy.csiv2 > layers > attributeLayer**

Determine the attribute layer options that are claimed by the server for incoming CSIV2 requests.

false

Attribute name	Data type	Default value	Description
identityAssertionEnabled	boolean	false	Indicate by true or false whether identity assertion is enabled. Default is false.
trustedIdentities	string		Specify a pipe ( )-separated list of server identities, which are trusted to perform identity assertion to this server. A value of "*" is also accepted to indicate implicit trust (trust anyone).

#### **serverPolicy.csiv2 > layers > attributeLayer > identityAssertionTypes**

Specify the supported identity token types for identity assertion.

false

#### **serverPolicy.csiv2 > layers > authenticationLayer**

Determine the authentication mechanisms and association options that are claimed by the server for incoming CSIV2 requests.

false

Attribute name	Data type	Default value	Description
establishTrustInClient	<ul style="list-style-type: none"><li>• Required</li><li>• Never</li><li>• Supported</li></ul>	Required	<p>Specify if this association option is Supported, Required, or Never used for this layer. It indicates authentication requirements at the authentication layer.</p> <p><b>Required</b> The association option is required</p> <p><b>Never</b> The association option must not be used</p> <p><b>Supported</b> The association option is supported</p>

**serverPolicy.csiv2 > layers > authenticationLayer > mechanisms**

Specifies authentication mechanisms as a comma separated list. For example: GSSUP, LTPA

false

string

**serverPolicy.csiv2 > layers > transportLayer**

Configure how to trust the client.

false

Attribute name	Data type	Default value	Description
sslEnabled	boolean	true	Indicate by true or false whether SSL is enabled for CSiv2 requests. Default is true and is the recommended value. If this attribute is set to false, sensitive information such as passwords and tokens are sent over unsecured channels when using IIOP.
sslRef	A reference to top level ssl element (string).		Specify the SSL configuration needed to establish a secure connection.

## OSGi Application (osgiApplication)

Defines the properties of an osgi application.

- application-bnd
  - security-role
  - group
  - run-as

- special-subject
- user

Attribute name	Data type	Default value	Description
autoStart	boolean	true	Indicates whether or not the server automatically starts the application.
id	string		A unique configuration ID.
location	A file, directory or url.		Location of an application expressed as an absolute path or a path relative to the server-level apps directory.
name	string		Name of an application.
suppressUncoveredHttpMethodWarning	boolean	false	Option to suppress uncovered HTTP method warning message during application deployment.

### application-bnd

Binds general deployment information included in the application to specific resources.

false

Attribute name	Data type	Default value	Description
version	string		Version of the application bindings specification.

### application-bnd > security-role

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Name of a security role.

### application-bnd > security-role > group

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		Group access ID
id	string		A unique configuration ID.
name	string		Name of a group possessing a security role.

### application-bnd > security-role > run-as

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
password	Reversably encoded password (string)		Password of a user required to access a bean from another bean. The value can be stored in clear text or encoded form. To encode the password, use the securityUtility tool with the encode option.
userid	string		ID of a user required to access a bean from another bean.

**application-bnd > security-role > special-subject**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
type	<ul style="list-style-type: none"> <li>• EVERYONE</li> <li>• ALL_AUTHENTICATED_USERS</li> </ul>		<p>One of the following special subject types: ALL_AUTHENTICATED_USERS, EVERYONE.</p> <p><b>EVERYONE</b> Everyone</p> <p><b>ALL_AUTHENTICATED_USERS</b> All authenticated users</p>

**application-bnd > security-role > user**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		A user access ID in the general form user:realmName/userUniqueId. A value will be generated if one is not specified.
id	string		A unique configuration ID.
name	string		Name of a user possessing a security role.

## OSGi Applications (osgiApplications)

Settings for all OSGi applications

Attribute name	Data type	Default value	Description
enable.debug	boolean	false	When this option is set to true, OSGi applications that fail to start remain installed to allow the application to be debugged.

## OSGi Library (osgiLibrary)

Enables OSGi applications to use packages provided by a shared library.

- library
  - file
  - fileset
  - folder
- package

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
libraryRef	A reference to top level library element (string).		The shared library reference to use for the OSGi library.

### library

The shared library reference to use for the OSGi library.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

### library > file

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

## package

A package export specification for a package that the system makes available for use by OSGi applications.

false

string

## Package (package)

The package configuration element.

Attribute name	Data type	Default value	Description
clusterName	string	default	The name of the cluster mapped to the package.
id	string		A unique configuration ID.
name	string	default	The name of the package.

## Persistent Scheduled Executor (persistentExecutor)

Schedules and runs persistent tasks.

- contextService
  - baseContext
    - baseContext
    - classloaderContext
    - jeeMetadataContext
    - securityContext
    - syncToOSThreadContext
    - zosWLMContext
  - classloaderContext
  - jeeMetadataContext
  - securityContext
  - syncToOSThreadContext
  - zosWLMContext

Attribute name	Data type	Default value	Description
contextServiceRef	A reference to top level contextService element (string).	DefaultContextService	Configures how context is captured and propagated to threads.
enableTaskExecution	boolean	true	Determines whether or not this instance may run tasks.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
initialPollDelay	A period of time with millisecond precision	0	Duration of time to wait before this instance might poll the persistent store for tasks to run. A value of -1 delays polling until it is started programmatically. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
pollInterval	A period of time with millisecond precision	-1	Interval between polling for tasks to run. A value of -1 disables all polling after the initial poll. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
pollSize	int Minimum: 1		The maximum number of task entries to find when polling the persistent store for tasks to run. If unspecified, there is no limit.
retryInterval	A period of time with millisecond precision	1m	The amount of time that must pass between the second and subsequent consecutive retries of a failed task. The first retry occurs immediately, regardless of the value of this attribute. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
retryLimit	short Minimum: -1 Maximum: 10000	10	Limit of consecutive retries for a task that has failed or rolled back, after which the task is considered permanently failed and does not attempt further retries. A value of -1 allows for unlimited retries.
taskStoreRef	A reference to top level databaseStore element (string).	defaultDatabaseStore	Persistent store for scheduled tasks.

### contextService

Configures how context is captured and propagated to threads.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**contextService > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

Attribute name	Data type	Default value	Description
baseContextRef	A reference to top level contextService element (string).		Specifies a base context service from which to inherit context that is not already defined on this context service.
id	string		A unique configuration ID.
jndiName	string		JNDI name

Attribute name	Data type	Default value	Description
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Determines the action to take in response to configuration errors. For example, if securityContext is configured for this contextService, but the security feature is not enabled, then onError determines whether to fail, raise a warning, or ignore the parts of the configuration which are incorrect.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>

**contextService > baseContext > baseContext**

Specifies a base context service from which to inherit context that is not already defined on this context service.

false

com.ibm.ws.context.service-factory

**contextService > baseContext > classloaderContext**

Classloader context propagation configuration.

false

**contextService > baseContext > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**contextService > baseContext > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**contextService > baseContext > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**contextService > baseContext > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"><li>• Propagate</li><li>• PropagateOrNew</li><li>• New</li></ul>	Propagate	<p>Indicates how the WLM context should be handled for non-Daemon work.</p> <p><b>Propagate</b> Use the same WLM Context (if one exists).</p> <p><b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists.</p> <p><b>New</b> Always create a new WLM context.</p>

**contextService > classloaderContext**

Classloader context propagation configuration.

false

**contextService > jeeMetadataContext**

Makes the namespace of the application component that submits a contextual task available to the task.

false

**contextService > securityContext**

When specified, the security context of the work initiator is propagated to the unit of work.

false

**contextService > syncToOSThreadContext**

When specified, the identity of the runAs Subject for the unit of work is synchronized with the Operating System identity.

false

**contextService > zosWLMContext**

Indicates that the z/OS WLM Context should be managed as part of the thread context.

false

Attribute name	Data type	Default value	Description
daemonTransactionClass	string	ASYNCDMN	The Transaction Class name provided to WLM to classify work when a new WLM context is created for Daemon work.
defaultTransactionClass	string	ASYNCBN	The Transaction Class name provided to WLM to classify work when a new WLM context is being created for non-Daemon work.
wlm	<ul style="list-style-type: none"> <li>• Propagate</li> <li>• PropagateOrNew</li> <li>• New</li> </ul>	Propagate	<p>Indicates how the WLM context should be handled for non-Daemon work.</p> <p><b>Propagate</b> Use the same WLM Context (if one exists).</p> <p><b>PropagateOrNew</b> Use the same WLM context or create a new one if no current context exists.</p> <p><b>New</b> Always create a new WLM context.</p>

## Web Server Plugin (pluginConfiguration)

Properties used when generating the web server plugin configuration file

- httpEndpoint
  - accessLogging
  - httpOptions
  - sslOptions
  - tcpOptions

Attribute name	Data type	Default value	Description
connectTimeout	A period of time with second precision	5s	Identifies the maximum amount of time that the application server should maintain a connection with the web server. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
extendedHandshake	boolean	false	If true, the web server plugin uses an extended handshake to determine if the application server is running.
httpEndpointRef	A reference to top level httpEndpoint element (string).	defaultHttpEndpoint	Specify the identifier of the http endpoint to include in the generated plugin-cfg.xml file. The endpoint defines the server in the cluster. The default value is 'defaultHttpEndpoint'.
ipv6Preferred	boolean	false	Used when resolving an application server host name of {null} or {0}, to prefer the type of address when possible
logDirLocation	Path to a directory		Deprecated: Identifies the directory where the http_plugin.log file is located. See Log file name.
logFileName	Path to a file	\${pluginInstallRoot}/logs/\${webserverName}/http_plugin.log	A fully qualified path to to the web server plug-in log file. Directory component must already exist. For Apache-based web servers, a path that begins with a pipe character is interpreted as an external piped logger. If specified, the path overrides logDirLocation.
pluginInstallRoot	string	/opt/IBM/WebSphere/Plugins	Web server plugin installation location in file system of web server host
serverIOTimeout	A period of time with second precision	900s	Identifies the maximum amount of time that the web server plugin waits to send a request or receive a response from the application server. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
serverIOTimeoutRetry	int Minimum: -1 Maximum: 65535	-1	Limits the number of request retries after a read or write timeout. The default value, {-1}, applies no additional limits, so retries are limited by the number of available servers in the cluster. A {0} value indicates there should be no retries. This value is scoped to the server cluster and does not apply to connection failures or timeouts due to the HTTP plug-in Connection timeout, or to web socket timeouts.
sslCertlabel	string		Specifies the label of the certificate within the keyring that the plug-in is to use when the web container requests a client certificate from the plug-in.
sslKeyringLocation	string	\${pluginInstallRoot}/ config/\${webserverName}/ plugin-key.kdb	The fully qualified path to the SSL keyring file on the web server host
sslStashfileLocation	string	\${pluginInstallRoot}/ config/\${webserverName}/ plugin-key.sth	The fully qualified path to the SSL stashfile on the web server host
waitForContinue	boolean	false	If false (the default value), the web server plugin sends the "Expect: 100-continue" header with HTTP requests that have a message body. When set to true, the web server plugin sends the "Expect: 100-continue" header with every HTTP request. Consider setting this value to true if you have a firewall between the web server and the application server, and are sensitive to requests retries with no request body.
webserverName	string	webserver1	Name of the web server where this configuration will be used. Used to generate the plugin log file location if that is not specified explicitly by Log file name or directory.

Attribute name	Data type	Default value	Description
webservicePort	int Minimum: -1 Maximum: 65535	80	Web server HTTP port
webserviceSecurePort	int Minimum: -1 Maximum: 65535	443	Web server HTTPS port
wsServerIOTimeout	A period of time with second precision		Identifies the maximum amount of time that the web server plugin waits to send a request or receive a websocket response from the application server. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
wsServerIdleTimeout	A period of time with second precision		Identifies the maximum amount of time that the web server plugin waits to terminate an idle websocket connection. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

### httpEndpoint

Specify the identifier of the http endpoint to include in the generated plugin-cfg.xml file. The endpoint defines the server in the cluster. The default value is 'defaultHttpEndpoint'.

false

Attribute name	Data type	Default value	Description
accessLoggingRef	A reference to top level httpAccessLogging element (string).		HTTP access logging configuration for the endpoint.
enabled	boolean	true	Toggle the availability of an endpoint. When true, this endpoint will be activated by the dispatcher to handle HTTP requests.

Attribute name	Data type	Default value	Description
host	string	localhost	IP address, domain name server (DNS) host name with domain name suffix, or just the DNS host name, used by a client to request a resource. Use '*' for all available network interfaces.
httpOptionsRef	A reference to top level httpOptions element (string).	defaultHttpOptions	HTTP protocol options for the endpoint.
httpPort	int Minimum: -1 Maximum: 65535		The port used for client HTTP requests. Use -1 to disable this port.
httpsPort	int Minimum: -1 Maximum: 65535		The port used for client HTTP requests secured with SSL (https). Use -1 to disable this port.
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Action to take after a failure to start an endpoint.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>
sslOptionsRef	A reference to top level sslOptions element (string).		SSL protocol options for the endpoint.
tcpOptionsRef	A reference to top level tcpOptions element (string).	defaultTCPOptions	TCP protocol options for the endpoint.

### httpEndpoint > accessLogging

HTTP access logging configuration for the endpoint.

false

Attribute name	Data type	Default value	Description
enabled	boolean	true	Enable access logging.

Attribute name	Data type	Default value	Description
filePath	Path to a file	\${server.output.dir}/logs/http_access.log	Directory path and name of the access log file. Standard variable substitutions, such as \${server.output.dir}, can be used when specifying the directory path.
logFormat	string	%h %u %{t}W "%r" %s %b	Specifies the log format that is used when logging client access information.
maxFileSize	int Minimum: 0	20	Maximum size of a log file, in megabytes, before being rolled over; a value of 0 means no limit.
maxFiles	int Minimum: 0	2	Maximum number of log files that will be kept, before the oldest file is removed; a value of 0 means no limit.

#### httpEndpoint > httpOptions

HTTP protocol options for the endpoint.

false

Attribute name	Data type	Default value	Description
keepAliveEnabled	boolean	true	Enables persistent connections (HTTP keepalive). If true, connections are kept alive for reuse by multiple sequential requests and responses. If false, connections are closed after the response is sent.
maxKeepAliveRequests	int Minimum: -1	100	Maximum number of persistent requests that are allowed on a single HTTP connection if persistent connections are enabled. A value of -1 means unlimited.

Attribute name	Data type	Default value	Description
<code>persistTimeout</code>	A period of time with second precision	30s	Amount of time that a socket will be allowed to remain idle between requests. This setting only applies if persistent connections are enabled. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
<code>readTimeout</code>	A period of time with second precision	60s	Amount of time to wait for a read request to complete on a socket after the first read occurs. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
<code>removeServerHeader</code>	boolean	false	Removes server implementation information from HTTP headers and also disables the default Liberty profile welcome page.
<code>writeTimeout</code>	A period of time with second precision	60s	Amount of time to wait on a socket for each portion of the response data to be transmitted. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**httpEndpoint > sslOptions**

SSL protocol options for the endpoint.

false

Attribute name	Data type	Default value	Description
sessionTimeout	A period of time with second precision	1d	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
sslRef	A reference to top level ssl element (string).		The default SSL configuration repertoire. The default value is defaultSSLSettings.
suppressHandshakeErrors	boolean	false	Disable logging of SSL handshake errors. SSL handshake errors can occur during normal operation, however these messages can be useful when SSL is behaving unexpectedly.

#### httpEndpoint > tcpOptions

TCP protocol options for the endpoint.

false

Attribute name	Data type	Default value	Description
inactivityTimeout	A period of time with millisecond precision	60s	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
soReuseAddr	boolean	true	Enables immediate rebind to a port with no active listener.

## Quick Start Security (quickStartSecurity)

Simple administrative security configuration.

Attribute name	Data type	Default value	Description
userName	string		Single user defined as part of the quick start security configuration. This user is granted the Administrator role.
userPassword	Reversably encoded password (string)		Password for the single user defined as part of the quick start security configuration. It is recommended that you encode this password. To do so, use the securityUtility tool with the encode option.

## Remote File Access (remoteFileAccess)

This element contains artifacts that control the level of file access exposed for remote connections.

- readDir
- writeDir

### readDir

A directory that remote clients are allowed to read from. There can be multiple readDir elements, and each represents a single directory that may refer to variables or absolute paths. Default is `#{wlp.install.dir}`, `#{wlp.user.dir}` and `#{server.output.dir}`

false

Path to a directory

### writeDir

A directory that remote clients are allowed to read from and write to. There can be multiple writeDir elements, and each represents a single directory that may refer to variables or absolute paths. Default is an empty set of directories.

false

Path to a directory

## Request Timing (requestTiming)

Provides warnings and diagnostic information for the slow or hung requests.

Attribute name	Data type	Default value	Description
hungRequestThreshold	A period of time with millisecond precision	10m	Duration of time that a request can run before being considered hung. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
includeContextInfo	boolean	true	Indicates if the context information details are included in the log output.
sampleRate	int Minimum: 1	1	Rate at which the sampling should happen for the slow request tracking. To sample one out of every n requests, set sampleRate to n. To sample all requests, set sampleRate to 1.
slowRequestThreshold	A period of time with millisecond precision	10s	Duration of time that a request can run before being considered slow. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

## Resource Adapter (resourceAdapter)

Defines a resource adapter installation.

- classloader
  - commonLibrary
    - file
    - fileset
    - folder
  - privateLibrary
    - file
    - fileset
    - folder

- customize

Attribute name	Data type	Default value	Description
autoStart	boolean		Configures whether a resource adapter starts automatically upon deployment of the resource adapter or lazily upon injection or lookup of a resource.
id	string		A unique configuration ID.
location	A file, directory or url.		Defines the path of the RAR file to install.
suppressUncoveredHttpMethodWarning	boolean	false	Option to suppress uncovered HTTP method warning message during application deployment.

### classloader

Defines the settings for an application classloader.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
classProviderRef	List of references to top level resourceAdapter elements (comma-separated string).		List of class provider references. When searching for classes or resources, this class loader will delegate to the specified class providers after searching its own class path.
commonLibraryRef	List of references to top level library elements (comma-separated string).		List of library references. Library class instances are shared with other classloaders.
delegation	<ul style="list-style-type: none"> <li>• parentFirst</li> <li>• parentLast</li> </ul>	parentFirst	Controls whether parent classloader is used before or after this classloader. If parent first is selected then delegate to immediate parent before searching the classpath. If parent last is selected then search the classpath before delegating to the immediate parent.  <b>parentFirst</b> Parent first  <b>parentLast</b> Parent last

Attribute name	Data type	Default value	Description
privateLibraryRef	List of references to top level library elements (comma-separated string).		List of library references. Library class instances are unique to this classloader, independent of class instances from other classloaders.

**classloader > commonLibrary**

List of library references. Library class instances are shared with other classloaders.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
id	string		A unique configuration ID.
name	string		Name of shared library for administrators

**classloader > commonLibrary > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**classloader > commonLibrary > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.

Attribute name	Data type	Default value	Description
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**classloader > commonLibrary > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**classloader > privateLibrary**

List of library references. Library class instances are unique to this classloader, independent of class instances from other classloaders.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
id	string		A unique configuration ID.
name	string		Name of shared library for administrators

**classloader > privateLibrary > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**classloader > privateLibrary > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**classloader > privateLibrary > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**customize**

Customizes the configuration properties element for the activation specification, administered object, or connection factory with the specified interface and/or implementation class.

false

Attribute name	Data type	Default value	Description
implementation	string		Fully qualified implementation class name for which the configuration properties element should be customized.
interface	string		Fully qualified interface class name for which the configuration properties element should be customized.

Attribute name	Data type	Default value	Description
suffix	string		Overrides the default suffix for the configuration properties element. For example, "CustomConnectionFactory" in properties.rarModule1.CustomConnectionFactory. The suffix is useful to disambiguate when multiple types of connection factories, administered objects, or endpoint activations are provided by a resource adapter. If a configuration properties element customization omits the suffix or leaves it blank, no suffix is used.

## Real-Time Communications (rtcomm)

Defines the configuration that is related to the Rtcomm feature and all its related components. All the real-time capabilities associated with the Rtcomm feature are configured under this single entity.

- callQueue
- gateway
  - allowFromSipEndpoint
    - sslOptions
    - tcpOptions
- iceServerURL

Attribute name	Data type	Default value	Description
alternateEndpointRoutingEnabled	boolean	false	Enables the alternate endpoint routing option. Administrators that want to control endpoint routing must enable this option.
messageServerHost	string	localhost	The host of the MQTT broker. The specified host can be an IP address or domain name server (DNS) hostname.
messageServerPort	int	1883	The port the MQTT broker listens on. The port is any valid port number.

Attribute name	Data type	Default value	Description
rtcommTopicPath	string	/rtcomm/	The MQTT topic path that is associated with this feature. All Rtcomm topic names configured within Rtcomm Options are prepended with this path. To create a unique name space for this Rtcomm instance within a message broker, modify this path to be unique.
sharedSubscriptionPath	string		Specifies the shared subscription path that is prepended to the topic path. This path is required by message brokers when using shared subscriptions.
sslEnabled	boolean	false	Uses SSL between the Rtcomm feature and the MQTT broker.
sslRef	A reference to top level ssl element (string).		ID of the SSL configuration to be used to connect to the SSL-enabled MQTT broker.

### callQueue

Defines a single instance of a call queue. This instance fully encapsulates all the configuration related to a single queue.

false

Attribute name	Data type	Default value	Description
callQueueID	string	callQueueID	The name that is associated with the call queue topic. This is the destination endpoint ID that a caller uses to call into a specific queue.
description	string		Specifies the description of this call queue instance. This description is returned in service query responses and can be used to better inform the client about the queue.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
timeout	A period of time with second precision	600s	The number of seconds to wait before terminating a call that is waiting in this queue. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

### gateway

A WebRTC gateway that provides connectivity from Rtcomm to SIP networks

false

Attribute name	Data type	Default value	Description
allowFromSipEndpointRef	List of references to top level sipEndpoint elements (comma-separated string).	defaultSipUAEndpoint	List of SIP endpoints for this connector.
externalPR	string		Host:port address of a SIP Proxy/Registrar. If assigned, all outgoing SIP messages are forwarded to this address
sipContainer	boolean	false	Outgoing SIP messages are routed to SIP applications installed locally

### gateway > allowFromSipEndpoint

List of SIP endpoints for this connector.

false

Attribute name	Data type	Default value	Description
bindRetries	int	60	The number of retries that are attempted when port binding is unsuccessful.
bindRetryDelay	A period of time with millisecond precision	5000ms	The delay between retries in milliseconds. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
host	string	localhost	The IP of the endpoint host
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
sipTCPPort	int	5060	The TCP port number
sipTLSport	int	5061	The TLS port number
sipUDPPort	int	5060	The UDP port number
sslOptionsRef	A reference to top level sslOptions element (string).		Defines SSL protocol settings
tcpOptionsRef	A reference to top level tcpOptions element (string).	defaultTCPOptions	Defines TCP protocol settings

**gateway > allowFromSipEndpoint > sslOptions**

Defines SSL protocol settings

false

Attribute name	Data type	Default value	Description
sessionTimeout	A period of time with second precision	1d	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
sslRef	A reference to top level ssl element (string).		The default SSL configuration repertoire. The default value is defaultSSLSettings.
suppressHandshakeErrors	boolean	false	Disable logging of SSL handshake errors. SSL handshake errors can occur during normal operation, however these messages can be useful when SSL is behaving unexpectedly.

**gateway > allowFromSipEndpoint > tcpOptions**

Defines TCP protocol settings

false

Attribute name	Data type	Default value	Description
inactivityTimeout	A period of time with millisecond precision	60s	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
soReuseAddr	boolean	true	Enables immediate rebind to a port with no active listener.

#### iceServerURL

Specifies the Interactive Connectivity Establishment (ICE) Server URL(s) available for client use. The client can request the list of ICE Server URL(s) for use with WebRTC by using an Rtcomm service query. This following is an example format for an ICE Server URL: - stun:hostname:port.

false

string

### SAF Authorization (safAuthorization)

Controls the security credential domain for SAF.

Attribute name	Data type	Default value	Description
enableDelegation	boolean	false	Enable RunAs delegation via SAF EJBROLE profiles.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
racRouteLog	<ul style="list-style-type: none"> <li>• NOSTAT</li> <li>• ASIS</li> <li>• NOFAIL</li> <li>• NONE</li> </ul>	NONE	<p>Specifies the types of access attempts to log.</p> <p><b>NOSTAT</b> The attempt is not recorded. No logging occurs and no resource statistics are updated.</p> <p><b>ASIS</b> Records the event in the manner specified in the profile that protects the resource, or by other methods such as the SETROPTS option.</p> <p><b>NOFAIL</b> If the authorization check fails, the attempt is not recorded. If the authorization check succeeds, the attempt is recorded as in ASIS.</p> <p><b>NONE</b> The attempt is not recorded.</p>
roleMapper	string	com.ibm.ws.security.authorization.OGSAuthorizationSAFRoleMapperImpl	OGSAuthorizationSAFRoleMapperImpl the SAF role mapper service provider.

## SAF Credentials (safCredentials)

Controls the operation of the SAF credentials.

Attribute name	Data type	Default value	Description
mapDistributedIdentities	boolean		Use distributed identity filters to map the distributed identities to SAF user IDs.
profilePrefix	string	BBGZDFLT	Profile prefix used to specify the SAF APPL-ID when creating SAF credentials and authorizing users against SAF resource profiles.
unauthenticatedUser	string	WSGUEST	SAF user ID of the unauthenticated user.

## SAF User Registry (safRegistry)

Configuration properties for a SAF user registry.

Attribute name	Data type	Default value	Description
enableFailover	boolean	true	Enable failover from authorized SAF services (e.g. initACEE) to unauthorized USS services (e.g. __passwd) if the server does not have access to the WLP z/OS System Security Access Domain.
realm	string		The realm name represents the user registry.

## SAF Role Mapper (safRoleMapper)

Defines how to generate SAF EJBROLE resource profile names from application role names.

Attribute name	Data type	Default value	Description
profilePattern	string	%profilePrefix%.%resource%.%role%	Pattern to use for generating EJBROLE resource profile names from application role names.
toUpperCase	boolean	false	Convert EJBROLE resource profile name to uppercase.

## SAML Web SSO 2.0 Authentication (samlWebSso20)

Controls the operation of the Security Assertion Markup Language Web SSO 2.0 Mechanism.

- audiences
- authFilter
  - host
  - remoteAddress
  - requestUrl
  - userAgent
  - webApp
- authnContextClassRef
- headerName
- pkixTrustEngine
  - crl
  - trustedIssuers
  - x509Certificate

Attribute name	Data type	Default value	Description
allowCreate	boolean		Allow the IdP to create a new account if the requesting user does not have one.

Attribute name	Data type	Default value	Description
allowCustomCacheKey	boolean	true	Allow generating a custom cache key to access the authentication cache and get the subject.
authFilterRef	A reference to top level authFilter element (string).		Specifies the authentication filter reference.
authnContextComparisonType	<ul style="list-style-type: none"> <li>• minimum</li> <li>• better</li> <li>• maximum</li> <li>• exact</li> </ul>	exact	<p>When an authnContextClassRef is specified, the authnContextComparisonType can be set.</p> <p><b>minimum</b> Minimum. The authentication context in the authentication statement must be at least as strong as one of the authentication contexts specified.</p> <p><b>better</b> Better. The authentication context in the authentication statement must be stronger than any one of the authentication contexts specified.</p> <p><b>maximum</b> Maximum. The authentication context in the authentication statement must be as strong as possible without exceeding the strength of at least one of the authentication contexts specified.</p> <p><b>exact</b> Exact. The authentication context in the authentication statement must be an exact match of at least one of the authentication contexts specified.</p>

Attribute name	Data type	Default value	Description
authnRequestTime	A period of time with millisecond precision	10m	Specifies the life time period of an authnRequest which is generated and sent from the service provider to an IdP for requesting a SAML Token. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
authnRequestsSigned	boolean	true	Indicates whether the <samlp:AuthnRequest> messages sent by this service provider will be signed.
clockSkew	A period of time with millisecond precision	5m	This is used to specify the allowed clock skew in minutes when validating the SAML token. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
createSession	boolean	true	Specifies whether to create an HttpSession if the current HttpSession does not exist.
customizeNameIDFormat	string		Specifies the customized URI reference corresponding to a name identifier format that is not defined in the SAML core specification.
disableLtpaCookie	boolean	true	Do not create an LTPA Token during processing of the SAML Assertion. Create a cookie of the specific Service Provider instead.
enabled	boolean	true	The service provider is enabled if true and disabled if false.

Attribute name	Data type	Default value	Description
errorPageURL	string		Specifies an error page to be displayed if the SAML validation fails. If this attribute is not specified, and the received SAML is invalid, the user will be redirected back to the SAML IdP to restart SSO.
forceAuthn	boolean	false	Indicates whether the IdP should force the user to re-authenticate.
groupIdIdentifier	string		Specifies a SAML attribute that is used as the name of the group that the authenticated principal is a member of. There is no default value.
httpsRequired	boolean	true	Enforce using SSL communication when accessing a SAML WebSSO service provider end point such as acs or metadata.
id	string		A unique configuration ID.
idpMetadata	string	`\${server.config.dir}/resources/security/idpMetadata.xml`	Specifies the IdP metadata file.
inboundPropagation	<ul style="list-style-type: none"> <li>• none</li> <li>• required</li> </ul>	none	<p>Controls the operation of the Security Assertion Markup Language Web SSO 2.0 for the inbound propagation of the Web Services Mechanisms.</p> <p><b>none</b>   %inboundPropagation.none  <b>required</b>   %inboundPropagation.required</p>
includeTokenInSubject	boolean	true	Specifies whether to include a SAML assertion in the subject.
includeX509InSPMetadata	boolean	true	Specifies whether to include the x509 certificate in the Liberty SP metadata.
isPassive	boolean	false	Indicates IdP must not take control of the end user interface.
keyAlias	string		Key alias name to locate the private key for signing and decryption. This is optional if the keystore has exactly one key entry, or if it has one key with an alias of 'samlsp'.

Attribute name	Data type	Default value	Description
keyStoreRef	A reference to top level keyStore element (string).		A keystore containing the private key for the signing of the AuthnRequest, and the decryption of EncryptedAssertion element. The default is the server's default.
loginPageURL	string		Specifies the SAML IdP login application URL to which an unauthenticated request is redirected. This attribute triggers IdP-initiated SSO, and it is only required for IdP-initiated SSO.
mapToUserRegistry	<ul style="list-style-type: none"> <li>• User</li> <li>• No</li> <li>• Group</li> </ul>	No	<p>Specifies how to map an identity to a registry user. The options are No, User, and Group. The default is No, and the user registry is not used to create the user subject.</p> <p><b>User</b> Map a SAML identity to a user defined in the registry</p> <p><b>No</b> Do not map a SAML identity to a user or group in the registry</p> <p><b>Group</b> Map a SAML identity to a group defined in the user registry</p>

Attribute name	Data type	Default value	Description
nameIDFormat	<ul style="list-style-type: none"> <li>• encrypted</li> <li>• customize</li> <li>• persistent</li> <li>• x509SubjectName</li> <li>• email</li> <li>• transient</li> <li>• entity</li> <li>• unspecified</li> <li>• kerberos</li> <li>• windowsDomainQualifiedName</li> </ul>	email	<p>Specifies the URI reference corresponding to a name identifier format defined in the SAML core specification.</p> <p><b>encrypted</b> urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted</p> <p><b>customize</b> Customized Name ID Format.</p> <p><b>persistent</b> urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</p> <p><b>x509SubjectName</b> urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</p> <p><b>email</b> urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</p> <p><b>transient</b> urn:oasis:names:tc:SAML:2.0:nameid-format:transient</p> <p><b>entity</b> urn:oasis:names:tc:SAML:2.0:nameid-format:entity</p> <p><b>unspecified</b> urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</p> <p><b>kerberos</b> urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</p> <p><b>windowsDomainQualifiedName</b> urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</p>
reAuthnCushion	A period of time with millisecond precision	0m	<p>The time period to authenticate again when a SAML Assertion is about to expire, which is indicated by either the statement NotOnOrAfter or the attribute SessionNotOnOrAfter of the SAML Assertion. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.</p>

Attribute name	Data type	Default value	Description
reAuthnOnAssertionExpire	boolean	false	Authenticate the incoming HTTP request again when a SAML Assertion is about to expire.
realmIdentifier	string		Specifies a SAML attribute that is used as the realm name. If no value is specified, the Issuer SAML assertion element value is used.
realmName	string		Specifies a realm name when mapToUserRegistry is set to No or Group.
sessionNotOnOrAfter	A period of time with millisecond precision	120m	Indicates an upper bound on SAML session durations, after which the Liberty SP should ask the user to re-authenticate to the IdP. If the SAML token returned from the IdP does not contain a sessionNotOnOrAfter assertion, the value specified by this attribute is used. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
signatureMethodAlgorithm	<ul style="list-style-type: none"> <li>• SHA256</li> <li>• SHA128</li> <li>• SHA1</li> </ul>	SHA256	<p>Indicates the required algorithm by this service provider.</p> <p><b>SHA256</b> SHA-256 signature algorithm</p> <p><b>SHA128</b> %signatureMethodAlgorithm.SHA128</p> <p><b>SHA1</b> SHA-1 signature algorithm</p>
spHostAndPort	string		Specifies a SAML service provider host name and port number.
targetPageUrl	string		The default landing page for the IdP-initiated SSO if the relayState is missing.

Attribute name	Data type	Default value	Description
tokenReplayTimeout	A period of time with millisecond precision	30m	This property is used to specify how long the Liberty SP should prevent token replay. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
userIdentifier	string		Specifies a SAML attribute that is used as the user principal name in the subject. If no value is specified, the NameID SAML assertion element value is used.
userUniqueIdentifier	string		Specifies a SAML attribute that is used as the unique user name as it applies to the WSCredential in the subject. The default is the same as the userIdentifier attribute value.
wantAssertionsSigned	boolean	true	Indicates a requirement for the <saml:Assertion> elements received by this service provider to be signed.

### audiences

The list of audiences which are trusted to verify the audience of the SAML Token. If the value is "ANY", then all audiences are trusted.

false

string

### authFilter

Specifies the authentication filter reference.

false

#### authFilter > host

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
name	string		Specifies the name.

**authFilter > remoteAddress**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
ip	string		Specifies the IP address.
matchType	<ul style="list-style-type: none"> <li>• lessThan</li> <li>• equals</li> <li>• greaterThan</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>lessThan</b> Less than <b>equals</b> Equals <b>greaterThan</b> Greater than <b>contains</b> Contains <b>notContain</b> Not contain

**authFilter > requestUrl**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
urlPattern	string		Specifies the URL pattern.

**authFilter > userAgent**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
agent	string		Specifies the user agent
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain

#### **authFilter > webApp**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
name	string		Specifies the name.

#### **authnContextClassRef**

A URI reference identifying an authentication context class that describes the authentication context declaration. The default is null.

false

string

#### **headerName**

The header name of the HTTP request which stores the SAML Token.

false

string

#### **pkixTrustEngine**

Specifies the PKIX trust information that is used to evaluate the trustworthiness and validity of XML signatures in a SAML response. Do not specify multiple pkixTrustEngine in a samlWebSso20.

false

Attribute name	Data type	Default value	Description
trustAnchorRef	A reference to top level keyStore element (string).		A keystore containing the public key necessary for verifying the signature of the SAMLResponse and Assertion.

#### **pkixTrustEngine > crl**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
path	string		Specifies the path to the crl.

#### **pkixTrustEngine > trustedIssuers**

Specifies the identities of trusted IdP issuers. If the value is "ALL\_ISSUERS", then all IdP identities are trusted.

false

string

#### **pkixTrustEngine > x509Certificate**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
path	string		Specifies the path to the x509 certificate.

## **Scaling Definitions (scalingDefinitions)**

Defines the policies for the scaling controller

- defaultScalingPolicy
  - hostGroup
  - in
  - metric
  - out
- scalingPolicy
  - bind
  - hostGroup
  - in
  - metric
  - out

#### **defaultScalingPolicy**

Defines default criteria for starting or stopping Liberty servers based on demand for resources

false

Attribute name	Data type	Default value	Description
enabled	boolean	true	Indicates whether the scaling policy is enabled
max	int Minimum: -1	-1	Maximum number of cluster members that can be running at the same time
min	int Minimum: 0	2	Minimum number of cluster members to start

Attribute name	Data type	Default value	Description
name	<ul style="list-style-type: none"> <li>vertical</li> <li>horizontal</li> </ul>	horizontal	Indicates whether to scale horizontally or vertically. <b>vertical</b> Vertical <b>horizontal</b> Horizontal

#### **defaultScalingPolicy > hostGroup**

Defines criteria for determining which hosts can be used to provision new cluster members.

false

Attribute name	Data type	Default value	Description
tags	string		A space-delimited list of administrative metadata tags. A host is eligible to provision new cluster members if it has one of the tags.

#### **defaultScalingPolicy > in**

Defines detailed controls for reducing the number of servers

false

Attribute name	Data type	Default value	Description
amount	int Minimum: 1	1	The amount by which to scale, in the units defined by the units attribute.
minInterval	A period of time with millisecond precision	15m	The minimum amount of time between a scaling change. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
units	<ul style="list-style-type: none"> <li>percentage</li> <li>instance</li> </ul>	instance	The units by which to scale. <b>percentage</b> Amount is a percentage relative to the current number of instances. <b>instance</b> Amount is a number of instances.

**defaultScalingPolicy > metric**

Defines resource usage criteria for starting or removing a server

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
max	int Minimum: 0 Maximum: 100	90	The average percentage of the metric above which to scale out
min	int Minimum: 0 Maximum: 100	30	The average percentage of the metric below which to scale in
name	<ul style="list-style-type: none"> <li>• heap</li> <li>• cpu</li> <li>• memory</li> </ul>		Name of the scaling policy <b>heap</b> Heap <b>cpu</b> CPU <b>memory</b> Memory

**defaultScalingPolicy > out**

Defines detailed controls for increasing the number of servers

false

Attribute name	Data type	Default value	Description
amount	int Minimum: 1	1	The amount by which to scale, in the units defined by the units attribute.
minInterval	A period of time with millisecond precision	5m	The minimum amount of time between a scaling change. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
units	<ul style="list-style-type: none"> <li>percentage</li> <li>instance</li> </ul>	instance	<p>The units by which to scale.</p> <p><b>percentage</b> Amount is a percentage relative to the current number of instances.</p> <p><b>instance</b> Amount is a number of instances.</p>

### scalingPolicy

Defines criteria for starting or stopping Liberty servers based on demand for resources

false

Attribute name	Data type	Default value	Description
enabled	boolean	true	Indicates whether the scaling policy is enabled
id	string		A unique configuration ID.
max	int Minimum: -1	-1	Maximum number of cluster members that can be running at the same time
min	int Minimum: 0	2	Minimum number of cluster members to start
name	<ul style="list-style-type: none"> <li>vertical</li> <li>horizontal</li> </ul>	horizontal	<p>Indicates whether to scale horizontally or vertically.</p> <p><b>vertical</b> Vertical</p> <p><b>horizontal</b> Horizontal</p>

### scalingPolicy > bind

Defines the names of the clusters to which the policy is applied

false

Attribute name	Data type	Default value	Description
clusters	string		A comma-separated list of cluster names. A cluster name can be wildcarded with an asterisk at the end of the name only.

### scalingPolicy > hostGroup

Defines criteria for determining which hosts can be used to provision new cluster members.

false

Attribute name	Data type	Default value	Description
tags	string		A space-delimited list of administrative metadata tags. A host is eligible to provision new cluster members if it has one of the tags.

**scalingPolicy > in**

Defines detailed controls for reducing the number of servers

false

Attribute name	Data type	Default value	Description
amount	int Minimum: 1	1	The amount by which to scale, in the units defined by the units attribute.
minInterval	A period of time with millisecond precision	15m	The minimum amount of time between a scaling change. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
units	<ul style="list-style-type: none"> <li>• percentage</li> <li>• instance</li> </ul>	instance	<p>The units by which to scale.</p> <p><b>percentage</b> Amount is a percentage relative to the current number of instances.</p> <p><b>instance</b> Amount is a number of instances.</p>

**scalingPolicy > metric**

Defines resource usage criteria for starting or removing a server

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
max	int Minimum: 0 Maximum: 100		The average percentage of the metric above which to scale out

Attribute name	Data type	Default value	Description
min	int Minimum: 0 Maximum: 100		The average percentage of the metric below which to scale in
name	<ul style="list-style-type: none"> <li>• heap</li> <li>• cpu</li> <li>• memory</li> </ul>		Name of the scaling policy <b>heap</b> Heap <b>cpu</b> CPU <b>memory</b> Memory

### scalingPolicy > out

Defines detailed controls for increasing the number of servers

false

Attribute name	Data type	Default value	Description
amount	int Minimum: 1	1	The amount by which to scale, in the units defined by the units attribute.
minInterval	A period of time with millisecond precision	5m	The minimum amount of time between a scaling change. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
units	<ul style="list-style-type: none"> <li>• percentage</li> <li>• instance</li> </ul>	instance	The units by which to scale. <b>percentage</b> Amount is a percentage relative to the current number of instances. <b>instance</b> Amount is a number of instances.

## Scaling Member (scalingMember)

Defines the properties of a scaling member.

Attribute name	Data type	Default value	Description
metadataMonitorEnabled	boolean	false	Monitor the configuration directory for metadata file additions or updates, and publish to the collective controller.
metadataMonitorInterval	A period of time with millisecond precision	5s	Rate at which the server checks for metadata file additions or updates. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
metadataUpdateTrigger	<ul style="list-style-type: none"> <li>• timed</li> <li>• external</li> </ul>	timed	<p>Determines the method for triggering the update of metadata.</p> <p><b>timed</b> Server will scan for metadata changes at the polling interval and publish to the collective controller.</p> <p><b>external</b> Server will only update metadata when prompted by the FileNotificationMbean. The FileNotificationMbean is typically called by an external program such as an integrated development environment or a management application.</p>

## IBM SecureWay Directory Server LDAP Filters (securewayLdapFilterProperties)

Specifies the list of default IBM SecureWay Directory Server LDAP filters.

Attribute name	Data type	Default value	Description
groupFilter	string	(&(cn=%v)(!(objectclass=groupOfNames)(objectclass=groupOfUniqueNames)))	An LDAP filter clause for searching the user registry for groups.
groupIdMap	string	*:cn	An LDAP filter that maps the name of a group to an LDAP entry.
groupMemberIdMap	string	groupOfNames:member;groupOfUniqueNames:uniqueMember	An LDAP filter that identifies user to group memberships.
id	string		A unique configuration ID.
userFilter	string	(&(uid=%v)(objectclass=ePerson))	An LDAP filter clause for searching the user registry for users.
userIdMap	string	*:uid	An LDAP filter that maps the name of a user to an LDAP entry.

## Server Commands MBean (serverCommands)

Server Commands MBean configuration

Attribute name	Data type	Default value	Description
javadumpTimeout	A period of time with second precision	60s	Amount of time to wait for remote server to generate Java heap dump or thread dump. The default value is 60 seconds. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
startServerTimeout	A period of time with second precision	60s	Amount of time to wait for remote server to start. The default value is 60 seconds. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
stopServerTimeout	A period of time with second precision	60s	Amount of time to wait for remote server to stop. The default value is 60 seconds. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

## SIP Application Router (sipApplicationRouter)

Configuration for the SIP application router

Attribute name	Data type	Default value	Description
carProvider	string	*	The fully qualified domain name (FQDN) of the custom application router provider. Set to an asterisk (*) to use an arbitrary available provider.
enable.car	boolean	true	Applications are routed using the available custom application router; otherwise, the default application router is used.
sipDarConfiguration	Path to a file		The location of the default application router (DAR) properties file. This value is mapped to JSR 289 javax.servlet.sip.ar.dar.configuration. The DAR must be configured as specified in JSR 289.
sipNoRouteErrorCode	int	403	The error response code that is sent by the SIP container when no active servlet can be mapped to an incoming initial request.

## SIP Container (sipContainer)

Configuration for the SIP servlets container

- sipIntrospect
- sipTasksDispatcher

Attribute name	Data type	Default value	Description
dispatcherMessageQueueSize	int	1000	The maximum number of tasks that a SIP container queue can contain before it declares an overload state.
invalidateSessionOnShutdown	boolean	false	When the SIP container shuts down, the sessions are no longer valid. By default, sessions remain active until they expire.
markInternalResponse	boolean	false	Mark internally generated responses by setting the com.ibm.websphere.sip.container.internal.mark attribute on the response.
maxAppSessions	int	120000	The maximum number of SIP application sessions allowed at once.
maxMessageRate	int	5000	The maximum number of messages allowed per averaging period.
maxResponseTime	A period of time with millisecond precision	0ms	The maximum response time allowed in milliseconds. When set to 0, the response time is unlimited. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
messageQueueBurstFactor	int	10	The burst factor for the message queue size. The message queue size is set to (dispatcher message queue size) * (message queue burst factor). Setting a burst factor handles bursts in traffic by providing additional space in the queue before new messages are dropped.
msgArrivalTimeAttr	boolean	false	Save the message arrival time as an attribute of the message.

### sipIntrospect

Configuration for the SIP introspect

false

Attribute name	Data type	Default value	Description
method	<ul style="list-style-type: none"> <li>• VERBOSE</li> <li>• SUCCINCT</li> </ul>	SUCCINCT	<p>The level of SIP state details to include when generating server dump.</p> <p><b>VERBOSE</b> Includes the detailed state of the SIP application sessions and the SIP sessions in the server dump.</p> <p><b>SUCCINCT</b> Server dumps include only the SIP application sessions and SIP sessions IDs</p>

### sipTasksDispatcher

Configuration for the executor of parallel SIP tasks

false

Attribute name	Data type	Default value	Description
concurrentContainerTasks	int	15	The maximum number of concurrent SIP tasks that can be dispatched to the executor.

## SIP Endpoint (sipEndpoint)

Configuration for the SIP endpoint

- sslOptions
- tcpOptions

Attribute name	Data type	Default value	Description
bindRetries	int	60	The number of retries that are attempted when port binding is unsuccessful.
bindRetryDelay	A period of time with millisecond precision	5000ms	The delay between retries in milliseconds. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
host	string	localhost	The IP of the endpoint host
id	string		A unique configuration ID.
sipTCPPort	int	5060	The TCP port number

Attribute name	Data type	Default value	Description
sipTLSPort	int	5061	The TLS port number
sipUDPPort	int	5060	The UDP port number
sslOptionsRef	A reference to top level sslOptions element (string).		Defines SSL protocol settings
tcpOptionsRef	A reference to top level tcpOptions element (string).	defaultTCPOptions	Defines TCP protocol settings

### sslOptions

Defines SSL protocol settings

false

Attribute name	Data type	Default value	Description
sessionTimeout	A period of time with second precision	1d	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
sslRef	A reference to top level ssl element (string).		The default SSL configuration repertoire. The default value is defaultSSLSettings.
suppressHandshakeErrors	boolean	false	Disable logging of SSL handshake errors. SSL handshake errors can occur during normal operation, however these messages can be useful when SSL is behaving unexpectedly.

### tcpOptions

Defines TCP protocol settings

false

Attribute name	Data type	Default value	Description
inactivityTimeout	A period of time with millisecond precision	60s	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
soReuseAddr	boolean	true	Enables immediate rebind to a port with no active listener.

## SIP Stack (sipStack)

Configuration for the SIP stack

- commaSeparatedHeaders
- hideMessageHeaders
- sipQuotedParameters

Attribute name	Data type	Default value	Description
acceptNonUtf8Bytes	boolean	false	Accept byte sequences that are not encoded in UTF-8.
auto100OnInvite	boolean	true	The SIP container automatically sends a 100 response code when an INVITE request is received.
auto482OnMergedRequests	boolean	false	The SIP container automatically sends a 482 response code when a merged request is received. This behavior is defined in the SIP RFC 3261 Section 8.2.2.2.

Attribute name	Data type	Default value	Description
compactHeaders	<ul style="list-style-type: none"> <li>• API</li> <li>• Never</li> <li>• Always</li> <li>• MtuExceeds</li> </ul>	MtuExceeds	<p>Defines when the SIP stack uses compact headers when encoding a message.</p> <p><b>API</b> Headers are sent according to JSR289 <code>javax.servlet.sip.SipServletRequest</code>.</p> <p><b>Never</b> Headers are never sent in compact form</p> <p><b>Always</b> Headers are always sent in compact form</p> <p><b>MtuExceeds</b> Headers are sent in compact form only when MTU is exceeded</p>
forceConnectionReuse	boolean	true	Connections are reused in subsequent requests even if the alias parameter exists in the via header.
hideMessageBody	boolean	false	Hide message content in the SIP container logs.
hideMessageReqUri	boolean	false	Hide the message request URI in the SIP container logs.
networkAddressCacheTtl	string		The amount of time that the SIP container keeps a cached <code>InetAddress</code> entry and does not resolve it again.
pathMtu	int	1500	The maximum transmission unit (MTU) for outbound UDP requests, as defined in RFC 3261-18.1.1.
timerA	A period of time with millisecond precision	500ms	The initial INVITE request retransmit interval for UDP only, in milliseconds, as defined in RFC 3261. The default value equals T1. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
timerB	A period of time with millisecond precision	32000ms	The INVITE client transaction timeout timer, in milliseconds, as defined in RFC 3261. The default value equals 64*T1. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
timerD	A period of time with millisecond precision	32000ms	The wait time for INVITE response retransmits, in milliseconds, as defined in RFC 3261. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
timerE	A period of time with millisecond precision	500ms	The initial non-INVITE request retransmit interval for UDP only, in milliseconds, as defined in RFC 3261. The default value equals T1. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
timerF	A period of time with millisecond precision	32000ms	The non-INVITE transaction timeout timer, in milliseconds, as defined in RFC 3261. The default value equals $64 \cdot T1$ . Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
timerG	A period of time with millisecond precision	500ms	The initial INVITE response retransmit interval, in milliseconds, as defined in RFC 3261. The default value equals $T1$ . Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
timerH	A period of time with millisecond precision	32000ms	The wait time for ACK receipts, in milliseconds, as defined in RFC 3261. The default value equals $64 \cdot T1$ . Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
timerI	A period of time with millisecond precision	5000ms	The wait time for ACK retransmits, in milliseconds, as defined in RFC 3261. The default value equals T4. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
timerJ	A period of time with millisecond precision	32000ms	The wait time for non-INVITE request retransmits, in milliseconds, as defined in RFC 3261. The default value equals 64*T1. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
timerK	A period of time with millisecond precision	5000ms	The wait time for non-INVITE response retransmits, in milliseconds, as defined in RFC 3261. The default value equals T4. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

Attribute name	Data type	Default value	Description
timerT1	A period of time with millisecond precision	500ms	The round-trip time (RTT) estimate, in milliseconds, as defined in RFC 3261. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
timerT2	A period of time with millisecond precision	4000ms	The maximum retransmit interval, in milliseconds, for non-INVITE requests and INVITE responses, as defined in RFC 3261. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
timerT4	A period of time with millisecond precision	5000ms	The maximum duration that a message remains in the network in milliseconds, as defined in RFC 3261. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

#### **commaSeparatedHeaders**

A list of header fields that should be comma-separated. If there are multiple values of the same header, the headers are not duplicated and the value will be in the same header separated by a comma.

false

string

#### **hideMessageHeaders**

A comma-separated list of headers that is not output to the SIP container logs.

false

string

### sipQuotedParameters

A list of header parameters with values that are quoted.

false

string

## Spnego Authentication (spnego)

Controls the operation of the Simple and Protected GSS-API Negotiation Mechanism.

- authFilter
  - host
  - remoteAddress
  - requestUrl
  - userAgent
  - webApp

Attribute name	Data type	Default value	Description
authFilterRef	A reference to top level authFilter element (string).		Specifies the authentication filter reference.
canonicalHostName	boolean	true	Controls whether you want to use the canonical host name.
disableFailOverToAppAuthType	boolean	true	Specifies that SPNEGO is used to log in to WebSphere Application Server first. However, if the login fails, then the application authentication mechanism is used to log in to the WebSphere Application Server.
includeClientGSSCredentialInSubject	boolean	true	Specifies whether the client delegation credentials should be stored in a client subject.
krb5Config	string		Specifies the fully qualified Kerberos configuration path and name. Standard variable substitutions, such as \${server.config.dir}, can be used when specifying the directory path.

Attribute name	Data type	Default value	Description
krb5Keytab	string		Specifies the fully qualified Kerberos keytab path and name. Standard variable substitutions, such as <code>\${server.config.dir}</code> , can be used when specifying the directory path. The Kerberos keytab file contains a list of keys that are analogous to user passwords. It is important for hosts to protect their Kerberos keytab files by storing them on the local disk.
ntlmTokenReceivedErrorPageURL	URL		Specifies the URL of a resource that contains the content which SPNEGO includes in the HTTP response, which is displayed by the browser client application.
servicePrincipalNames	string		Specifies a list of Kerberos service principal names separated by a comma.
spnegoNotSupportedErrorPageURL	URL		Specifies the URL of a resource that contains the content which SPNEGO includes in the HTTP response that is displayed by the browser client application if it does not support SPNEGO authentication.
trimKerberosRealmNameFromPrincipal	boolean	true	Specifies whether SPNEGO removes the suffix of the Kerberos principal user name, starting from the <code>@</code> that precedes the Kerberos realm name. If this attribute is set to true, the suffix of the principal user name is removed. If this attribute is set to false, the suffix of the principal name is retained.

#### **authFilter**

Specifies the authentication filter reference.

false

#### **authFilter > host**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
name	string		Specifies the name.

**authFilter > remoteAddress**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
ip	string		Specifies the IP address.
matchType	<ul style="list-style-type: none"> <li>• lessThan</li> <li>• equals</li> <li>• greaterThan</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>lessThan</b> Less than <b>equals</b> Equals <b>greaterThan</b> Greater than <b>contains</b> Contains <b>notContain</b> Not contain

**authFilter > requestUrl**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
urlPattern	string		Specifies the URL pattern.

**authFilter > userAgent**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
agent	string		Specifies the user agent
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain

#### **authFilter > webApp**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
matchType	<ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> <li>• notContain</li> </ul>	contains	Specifies the match type. <b>equals</b> Equals <b>contains</b> Contains <b>notContain</b> Not contain
name	string		Specifies the name.

## SSL Repertoire (ssl)

An SSL repertoire with an ID, a defined keystore, and an optional truststore.

Attribute name	Data type	Default value	Description
clientAuthentication	boolean	false	Specifies whether client authentication is enabled. If set to true then client authentication is required and the client must provide a certificate for the server trusts.
clientAuthenticationSupported	boolean	false	Specifies whether a client authentication is supported. If set to true then the client authentication support means the server will check trust from a client if the client presents a certificate.

Attribute name	Data type	Default value	Description
clientKeyAlias	string		Specifies the alias of the certificate in the keystore that is used as the key to send to a server that has client authentication enabled. This attribute is only needed if the keystore has more than one key entry.
enabledCiphers	string		Specifies a custom list of ciphers. Separate each cipher in the list with a space. The supported cipher will depend on the underlying JRE used. Please check the JRE for valid ciphers.
id	string		A unique configuration ID.
keyStoreRef	A reference to top level keyStore element (string).		A keystore containing key entries for the SSL repertoire. This attribute is required.
securityLevel	<ul style="list-style-type: none"> <li>• MEDIUM</li> <li>• CUSTOM</li> <li>• HIGH</li> <li>• LOW</li> </ul>	HIGH	<p>Specifies the cipher suite group used by the SSL handshake. HIGH are 3DES and 128 bit and higher ciphers, MEDIUM are DES and 40 bit ciphers, LOW are ciphers without encryption. If the enabledCiphers attribute is used the securityLevel list is ignored.</p> <p><b>MEDIUM</b> %repertoire.MEDIUM</p> <p><b>CUSTOM</b> %repertoire.CUSTOM</p> <p><b>HIGH</b> Cipher suites 3DES and 128 bit and higher</p> <p><b>LOW</b> %repertoire.LOW</p>
serverKeyAlias	string		Specifies the alias of the certificate in the keystore used as the server's key. This attribute is only needed if the keystore has more then one key entry.

Attribute name	Data type	Default value	Description
sslProtocol	string		The SSL handshake protocol. Protocol values can be found in the documentation for the underlying JRE's Java Secure Socket Extension (JSSE) provider. When using the IBM JRE the default value is SSL_TLS and when using the Oracle JRE the default value is SSL.
trustStoreRef	A reference to top level keyStore element (string).	\${keyStoreRef}	A keystore containing trusted certificate entries used by the SSL repertoire for signing verification. This attribute is optional. If unspecified, the same keystore is used for both key and trusted certificate entries.

## SSL Default Repertoire (sslDefault)

The default repertoire for SSL services.

Attribute name	Data type	Default value	Description
sslRef	A reference to top level ssl element (string).	defaultSSLConfig	The name of the SSL repertoire that will be used as the default. The default SSL repertoire called defaultSSLConfig is used if none is specified.

## SSL Options (sslOptions)

The SSL protocol configuration for a transport.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
sessionTimeout	A period of time with second precision	1d	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
sslRef	A reference to top level ssl element (string).		The default SSL configuration repertoire. The default value is defaultSSLSettings.
suppressHandshakeErrors	boolean	false	Disable logging of SSL handshake errors. SSL handshake errors can occur during normal operation, however these messages can be useful when SSL is behaving unexpectedly.

## Stack Group (stackGroup)

The stack group configuration.

- deployVariable
- installable
- package

Attribute name	Data type	Default value	Description
deployVariableRef	List of references to top level deployVariable elements (comma-separated string).		The deploy variable configuration element.
electionPort	int	20020	The election port number to use for vertically deployed stack groups. Ensure all stacks deployed to the same host use the same election port.
id	string		A unique configuration ID.
installDir	Path to a directory		The target installation directory for user packages from this stack group. The default value is the /wlp.usr directory. Use a period (.) and not a slash (/ or \) before the usr sub-directory.
installableRef	List of references to top level installable elements (comma-separated string).		The installable configuration element
jreInstallDir	Path to a directory		The target installation directory for "jre" type installables from this stack group. The default value is the /wlp.jre directory. Use a period (.) and not a slash (/ or \) before the jre sub-directory.
name	string		Name for the stack group. The attribute has no default value.

Attribute name	Data type	Default value	Description
otherInstallDir	Path to a directory		The target installation directory for "other" type installables from this stack group. The default value is the /wlp.other directory. Use a period (.) and not a slash (/ or \) before the other sub-directory.
packageRef	List of references to top level package elements (comma-separated string).		The package configuration element.
transferTimeout	A period of time with second precision	10m	The maximum file transfer time in seconds to wait while transferring an individual file of this stack group to a target host. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
wlpInstallDir	Path to a directory		The target installation directory for "wlp" type installables from this stack group. The default value is the /wlp directory.

### deployVariable

The deploy variable configuration element.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
increment	int	0	Increment value for the deployVariable.
name	string		Name for the deployVariable.
value	string		Initial value of the deployVariable.

### installable

The installable configuration element

false

Attribute name	Data type	Default value	Description
expand	string		Specifies whether to expand the installable during deployment. Valid values are yes, no, or auto. Overrides the default behavior determined by the installable file type. A no value disables unzip for installable zip files. The default value is auto, which determines whether to expand or not expand based on the installable file type. For example, auto selects to expand the zip file type.
id	string		A unique configuration ID.
installDir	string		Absolute path to the installable target directory.
name	string	default	The name of the installable archive file, for example, wlp.8555.zip.
sourceDir	string		Absolute path to the installable archive file. The default value is the path: <code>\${WLP_STACK_GROUPS_DIR}/stack_name/installables</code>
type	string		The installable type. Valid values are wlp, jre, or other. This attribute overrides the type prefix of the installable name.

### package

The package configuration element.

false

Attribute name	Data type	Default value	Description
clusterName	string	default	The name of the cluster mapped to the package.
id	string		A unique configuration ID.
name	string	default	The name of the package.

## Stack Manager (stackManager)

The stack manager service configuration.

Attribute name	Data type	Default value	Description
controllerUser	string		The user ID of the controller to be used for this stack manager.

Attribute name	Data type	Default value	Description
controllerUserPassword	Reversably encoded password (string)		The password of the controller user to be used for this stack manager.
groupsDir	string		The directory containing the packages and installables for this stack manager.
id	string		A unique configuration ID.
scanningEnabled	boolean	true	Monitor the stack groups directory for additions, updates, and deletions.
scanningInterval	A period of time with millisecond precision	5000	The interval at which the controller will check for stack group additions, updates, and deletions. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

## Sync-to-OS-thread (syncToOSThread)

Enables and configures the Sync-to-OS-thread.

Attribute name	Data type	Default value	Description
appEnabled	boolean	false	Enable sync-to-OS-thread for applications.
id	string		A unique configuration ID.
j2cEnabled	boolean	false	Enable sync-to-OS-thread for j2c connectors that support native thread identity.

## TCP Options (tcpOptions)

Defines TCP protocol settings.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
inactivityTimeout	A period of time with millisecond precision	60s	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
soReuseAddr	boolean	true	Enables immediate rebind to a port with no active listener.
addressExcludeList	string		A list of addresses that are not allowed to make inbound connections on this channel. IPv4 or IPv6 addresses can be specified. All values in an IPv4 or IPv6 address must be represented by a number, or an asterisk that is used as a wildcard character.
addressIncludeList	string		A list of addresses that are allowed to make inbound connections on this channel. IPv4 or IPv6 addresses can be specified. All values in an IPv4 or IPv6 address must be represented by a number, or an asterisk that is used as a wildcard character.
hostNameExcludeList	string		A list of host names that are not allowed to make inbound connections on this channel. Host names can start with an asterisk, which is used as a wildcard character. However, an asterisk must not appear elsewhere in the address. For example, *.abc.com is valid, but *.abc.* is invalid.

Attribute name	Data type	Default value	Description
hostNameIncludeList	string		A list of host names that are allowed to make inbound connections on this channel. Host names can start with an asterisk, which is used as a wildcard character. However, an asterisk must not appear elsewhere in the address. For example, *.abc.com is valid, but *.abc.* is invalid.
maxOpenConnections	integer	128000	The maximum number of open connections per HTTP Endpoint. The range of possible values is between 1 and 1280000. This value is not strictly enforced to the exact value that is configured due to the timing of connections opening and closing.

For more information, see TCP transport channel settings.

## Timed Operation (timedOperation)

Timed operations help WebSphere Application Server administrators see when certain actions in their application server are operating more slowly than expected.

Attribute name	Data type	Default value	Description
enableReport	boolean	true	Enables periodic generation of report to the logs detailing the ten longest timed operations, grouped by type, and sorted within each group by expected duration
maxNumberTimedOperations	int	10000	A warning is logged when the total number of timed operations reaches this value.
reportFrequency	A period of time with hour precision		Frequency of generating report to the logs detailing the ten longest timed operations, grouped by type, and sorted within each group by average of actual duration. Specify a positive integer followed by the unit of time, which can be hours (h). For example, specify 12 hours as 12h.

## Transaction Manager (transaction)

Configuration properties for the Transaction Manager service

- dataSource
  - connectionManager
  - containerAuthData
  - jaasLoginContextEntry
  - jdbcDriver
    - library
      - file
      - fileset
      - folder
  - properties
  - properties.datadirect.sqlserver
  - properties.db2.i.native
  - properties.db2.i.toolbox
  - properties.db2.jcc
  - properties.derby.client
  - properties.derby.embedded
  - properties.informix
  - properties.informix.jcc
  - properties.microsoft.sqlserver
  - properties.oracle
  - properties.sybase
  - recoveryAuthData

Attribute name	Data type	Default value	Description
acceptHeuristicHazard	boolean	true	Specifies whether all applications on this server accept the possibility of a heuristic hazard occurring in a two-phase transaction that contains a one-phase resource.
clientInactivityTimeout	A period of time with second precision	60s	Maximum duration between transactional requests from a remote client. Any period of client inactivity that exceeds this timeout results in the transaction being rolled back in this application server. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
dataSourceRef	A reference to top level dataSource element (string).		This is an optional property. By default the transaction service stores its recovery logs in a file. As an alternative it is possible to store the logs in an RDBMS. This is achieved by setting this property which defines a non-transactional data source where the transaction logs will be stored.
defaultMaxShutdownDelay	A period of time with second precision	2s	Default maximum shutdown delay. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
enableLoggingForHeuristicReporting	boolean	false	Specifies whether the application server logs about-to-commit-one-phase-resource events from transactions that involve both a one-phase commit resource and two-phase commit resources.
heuristicRetryInterval	A period of time with second precision	60s	Amount of time that the application server waits before retrying a completion signal, such as commit or rollback, after a transient exception from a resource manager or remote partner. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
heuristicRetryWait	int	5	The number of times that the application server retries a completion signal, such as commit or rollback. Retries occur after a transient exception from a resource manager or remote partner.

Attribute name	Data type	Default value	Description
lpsHeuristicCompletion	<ul style="list-style-type: none"> <li>• COMMIT</li> <li>• MANUAL</li> <li>• ROLLBACK</li> </ul>	ROLLBACK	<p>Specifies the direction that is used to complete a transaction that has a heuristic outcome; either the application server commits or rolls back the transaction, or depends on manual completion by the administrator. Allowed values are: COMMIT, ROLLBACK and MANUAL</p> <p><b>COMMIT</b> Commit</p> <p><b>MANUAL</b> Manual</p> <p><b>ROLLBACK</b> Rollback</p>
propogatedOrBMTTranLifetime	Time period of time with second precision	0	Upper limit of the transaction timeout for transactions that run in this server. This value should be greater than or equal to the value specified for the total transaction timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
recoverOnStartup	boolean	false	Specifies whether the server should begin transaction recovery at server startup.
recoveryGroup	string		Name of the recovery group that this server belongs too. Members of a recovery group can recover the transaction logs of other servers in the group.
recoveryIdentity	string		Unique identity of this server for transaction peer recovery.
timeoutGracePeriodEnabled	boolean	false	Specifies whether there is a delay between a transaction timeout and the abnormal ending of the servant region that was running the transaction.

Attribute name	Data type	Default value	Description
totalTranLifetimeTimeout	A period of time with second precision	120s	Default maximum time allowed for transactions started on this server to complete. Any such transactions that do not complete before this timeout occurs are rolled back. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
transactionLogDBTableSuffix	string		When recovery logs are stored in an RDBMS table, this property allows the table name to be post-pended with a string to make it unique for this Server.
transactionLogDirectory	string	\${server.output.dir}/tranlog/	A directory for this server where the transaction service stores log files for recovery.
transactionLogSize	int	1024	Specifies the size of transaction log files in Kilobytes.
waitForRecovery	boolean	false	Specifies whether the server should wait for transaction recovery to complete before accepting new transactional work.

#### dataSource

This is an optional property. By default the transaction service stores its recovery logs in a file. As an alternative it is possible to store the logs in an RDBMS. This is achieved by setting this property which defines a non-transactional data source where the transaction logs will be stored.

false

Attribute name	Data type	Default value	Description
beginTranForResultSetScrolling	boolean	true	Attempt transaction enlistment when result set scrolling interfaces are used.
beginTranForVendorAPIs	boolean	true	Attempt transaction enlistment when vendor interfaces are used.

Attribute name	Data type	Default value	Description
commitOrRollbackOnCleanup	<ul style="list-style-type: none"> <li>• commit</li> <li>• rollback</li> </ul>		<p>Determines how to clean up connections that might be in a database unit of work (AutoCommit=false) when the connection is closed or returned to the pool.</p> <p><b>commit</b> Clean up the connection by committing.</p> <p><b>rollback</b> Clean up the connection by rolling back.</p>
connectionManagerRef	A reference to top level connectionManager element (string).		Connection manager for a data source.
connectionSharing	<ul style="list-style-type: none"> <li>• MatchOriginalRequest</li> <li>• MatchCurrentState</li> </ul>	MatchOriginalRequest	<p>Specifies how connections are matched for sharing.</p> <p><b>MatchOriginalRequest</b> When sharing connections, match based on the original connection request.</p> <p><b>MatchCurrentState</b> When sharing connections, match based on the current state of the connection.</p>
containerAuthDataRef	A reference to top level authData element (string).		Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

Attribute name	Data type	Default value	Description
enableConnectionCasting	boolean	false	Indicates that connections obtained from the data source should be castable to interface classes that the JDBC vendor connection implementation implements. Enabling this option incurs additional overhead on each getConnection operation. If vendor JDBC interfaces are needed less frequently, it might be more efficient to leave this option disabled and use Connection.unwrap(interface) only where it is needed.
isolationLevel	<ul style="list-style-type: none"> <li>• TRANSACTION_REPEATABLE_READ</li> <li>• TRANSACTION_READ_COMMITTED</li> <li>• TRANSACTION_SERIALIZABLE</li> <li>• TRANSACTION_READ_UNCOMMITTED</li> <li>• TRANSACTION_SNAPSHOT</li> </ul>		<p>Default transaction isolation level.</p> <p><b>TRANSACTION_REPEATABLE_READ</b> Dirty reads and non-repeatable reads are prevented; phantom reads can occur.</p> <p><b>TRANSACTION_READ_COMMITTED</b> Dirty reads are prevented; non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SERIALIZABLE</b> Dirty reads, non-repeatable reads and phantom reads are prevented.</p> <p><b>TRANSACTION_READ_UNCOMMITTED</b> Dirty reads, non-repeatable reads and phantom reads can occur.</p> <p><b>TRANSACTION_SNAPSHOT</b> Snapshot isolation for Microsoft SQL Server JDBC Driver and DataDirect Connect for JDBC driver.</p>

Attribute name	Data type	Default value	Description
jaasLoginContextEntryRef	A reference to top level jaasLoginContextEntry element (string).		JAAS login context entry for authentication.
jdbcDriverRef	A reference to top level jdbcDriver element (string).		JDBC driver for a data source.
jndiName	string		JNDI name for a data source.
queryTimeout	A period of time with second precision		Default query timeout for SQL statements. In a JTA transaction, syncQueryTimeoutWithTransactionTimeout can override this default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
recoveryAuthDataRef	A reference to top level authData element (string).		Authentication data for transaction recovery.
statementCacheSize	int Minimum: 0	10	Maximum number of cached statements per connection.
supplementalJDBCTrace	boolean		Supplements the JDBC driver trace that is logged when JDBC driver trace is enabled in bootstrap.properties. JDBC driver trace specifications include: com.ibm.ws.database.logwriter, com.ibm.ws.db2.logwriter, com.ibm.ws.derby.logwriter, com.ibm.ws.informix.logwriter, com.ibm.ws.oracle.logwriter, com.ibm.ws.sqlserver.logwriter, com.ibm.ws.sybase.logwriter
syncQueryTimeoutWithTransactionTimeout	boolean	false	Use the time remaining (if any) in a JTA transaction as the default query timeout for SQL statements.
transactional	boolean	true	Enable participation in transactions that are managed by the application server.

Attribute name	Data type	Default value	Description
type	<ul style="list-style-type: none"> <li>javax.sql.DataSource</li> <li>javax.sql.XADataSource</li> <li>javax.sql.ConnectionPoolDataSource</li> </ul>		Type of data source. <b>javax.sql.DataSource</b> javax.sql.DataSource <b>javax.sql.XADataSource</b> javax.sql.XADataSource <b>javax.sql.ConnectionPoolDataSource</b> javax.sql.ConnectionPoolDataSource

**dataSource > connectionManager**

Connection manager for a data source.

false

Attribute name	Data type	Default value	Description
agedTimeout	A period of time with second precision	-1	Amount of time before a physical connection can be discarded by pool maintenance. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
connectionTimeout	A period of time with second precision	30s	Amount of time after which a connection request times out. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxConnectionsPerThread	int Minimum: 0		Limits the number of open connections on each thread.

Attribute name	Data type	Default value	Description
maxIdleTime	A period of time with second precision	30m	Amount of time after which an unused or idle connection can be discarded during pool maintenance, if doing so does not reduce the pool below the minimum size. A value of -1 disables this timeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maxPoolSize	int Minimum: 0	50	Maximum number of physical connections for a pool. A value of 0 means unlimited.
minPoolSize	int Minimum: 0		Minimum number of physical connections to maintain in the pool. The pool is not pre-populated. Aged timeout can override the minimum.
numConnectionsPerThreadLocal	int Minimum: 0		Caches the specified number of connections for each thread.

Attribute name	Data type	Default value	Description
purgePolicy	<ul style="list-style-type: none"> <li>• ValidateAllConnections</li> <li>• FailingConnectionOnly</li> <li>• EntirePool</li> </ul>	EntirePool	<p>Specifies which connections to destroy when a stale connection is detected in a pool.</p> <p><b>ValidateAllConnections</b> When a stale connection is detected, connections are tested and those found to be bad are closed.</p> <p><b>FailingConnectionOnly</b> When a stale connection is detected, only the connection which was found to be bad is closed.</p> <p><b>EntirePool</b> When a stale connection is detected, all connections in the pool are marked stale, and when no longer in use, are closed.</p>
reapTime	A period of time with second precision	3m	Amount of time between runs of the pool maintenance thread. A value of -1 disables pool maintenance. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

**dataSource > containerAuthData**

Default authentication data for container managed authentication that applies when bindings do not specify an authentication-alias for a resource reference with res-auth=CONTAINER.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

**dataSource > jaasLoginContextEntry**

JAAS login context entry for authentication.

false

Attribute name	Data type	Default value	Description
loginModuleRef	List of references to top level jaasLoginModule elements (comma-separated string).	hashtable,userNameAndPassword,certificate,trustID	Word certificate trustID of a JAAS login module.
name	string		Name of a JAAS configuration entry.

**dataSource > jdbcDriver**

JDBC driver for a data source.

false

Attribute name	Data type	Default value	Description
javax.sql.ConnectionPoolDataSource	string		JDBC driver implementation of javax.sql.ConnectionPoolDataSource.
javax.sql.DataSource	string		JDBC driver implementation of javax.sql.DataSource.
javax.sql.XADataSource	string		JDBC driver implementation of javax.sql.XADataSource.
libraryRef	A reference to top level library element (string).		Identifies JDBC driver JARs and native files.

**dataSource > jdbcDriver > library**

Identifies JDBC driver JARs and native files.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

**dataSource > jdbcDriver > library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**dataSource > jdbcDriver > library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**dataSource > jdbcDriver > library > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**dataSource > properties**

List of JDBC vendor properties for the data source. For example, `databaseName="dbname" serverName="localhost" portNumber="50000"`.

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database.
databaseName	string		JDBC driver property: databaseName.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
serverName	string		Server where the database is running.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**dataSource > properties.datadirect.sqlserver**

Data source properties for the DataDirect Connect for JDBC driver for Microsoft SQL Server.

false

Attribute name	Data type	Default value	Description
JDBCBehavior	<ul style="list-style-type: none"> <li>• 1</li> <li>• 0</li> </ul>	0	JDBC driver property: JDBCBehavior. Values are: 0 (JDBC 4.0) or 1 (JDBC 3.0).  <b>1</b> JDBC 3.0 <b>0</b> JDBC 4.0
XATransactionGroup	string		JDBC driver property: XATransactionGroup.
XMLDescribeType	<ul style="list-style-type: none"> <li>• longvarbinary</li> <li>• longvarchar</li> </ul>		JDBC driver property: XMLDescribeType.  <b>longvarbinary</b> longvarbinary <b>longvarchar</b> longvarchar
accountingInfo	string		JDBC driver property: accountingInfo.
alternateServers	string		JDBC driver property: alternateServers.
alwaysReportTriggerResults	boolean		JDBC driver property: alwaysReportTriggerResults.
applicationName	string		JDBC driver property: applicationName.
authenticationMethod	<ul style="list-style-type: none"> <li>• ntlm</li> <li>• userIdPassword</li> <li>• kerberos</li> <li>• auto</li> </ul>		JDBC driver property: authenticationMethod.  <b>ntlm</b> ntlm <b>userIdPassword</b> userIdPassword <b>kerberos</b> kerberos <b>auto</b> auto
bulkLoadBatchSize	long		JDBC driver property: bulkLoadBatchSize.
bulkLoadOptions	long		JDBC driver property: bulkLoadOptions.
clientHostName	string		JDBC driver property: clientHostName.
clientUser	string		JDBC driver property: clientUser.

Attribute name	Data type	Default value	Description
codePageOverride	string		JDBC driver property: codePageOverride.
connectionRetryCount	int		JDBC driver property: connectionRetryCount.
connectionRetryDelay	A period of time with second precision		JDBC driver property: connectionRetryDelay. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
convertNull	int		JDBC driver property: convertNull.
databaseName	string		JDBC driver property: databaseName.
dateTimeInputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeInputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
dateTimeOutputParameterType	<ul style="list-style-type: none"> <li>• dateTime</li> <li>• dateTimeOffset</li> <li>• auto</li> </ul>		JDBC driver property: dateTimeOutputParameterType.  <b>dateTime</b> dateTime <b>dateTimeOffset</b> dateTimeOffset <b>auto</b> auto
describeInputParameters	<ul style="list-style-type: none"> <li>• describeIfString</li> <li>• noDescribe</li> <li>• describeIfDateTime</li> <li>• describeAll</li> </ul>		JDBC driver property: describeInputParameters.  <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll

Attribute name	Data type	Default value	Description
describeOutputParameters	<ul style="list-style-type: none"> <li>describeIfString</li> <li>noDescribe</li> <li>describeIfDateTime</li> <li>describeAll</li> </ul>		JDBC driver property: describeOutputParameters. <b>describeIfString</b> describeIfString <b>noDescribe</b> noDescribe <b>describeIfDateTime</b> describeIfDateTime <b>describeAll</b> describeAll
enableBulkLoad	boolean		JDBC driver property: enableBulkLoad.
enableCancelTimeout	boolean		JDBC driver property: enableCancelTimeout.
encryptionMethod	<ul style="list-style-type: none"> <li>loginSSL</li> <li>requestSSL</li> <li>SSL</li> <li>noEncryption</li> </ul>		JDBC driver property: encryptionMethod. <b>loginSSL</b> loginSSL <b>requestSSL</b> requestSSL <b>SSL</b> SSL <b>noEncryption</b> noEncryption
failoverGranularity	<ul style="list-style-type: none"> <li>disableIntegrityCheck</li> <li>atomicWithRepositioning</li> <li>nonAtomic</li> <li>atomic</li> </ul>		JDBC driver property: failoverGranularity. <b>disableIntegrityCheck</b> disableIntegrityCheck <b>atomicWithRepositioning</b> atomicWithRepositioning <b>nonAtomic</b> nonAtomic <b>atomic</b> atomic
failoverMode	<ul style="list-style-type: none"> <li>connect</li> <li>select</li> <li>extended</li> </ul>		JDBC driver property: failoverMode. <b>connect</b> connect <b>select</b> select <b>extended</b> extended
failoverPreconnect	boolean		JDBC driver property: failoverPreconnect.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
initializationString	string		JDBC driver property: initializationString.
insensitiveResultSetBufferSize	int		JDBC driver property: insensitiveResultSetBufferSize.

Attribute name	Data type	Default value	Description
javaDoubleToString	boolean		JDBC driver property: javaDoubleToString.
loadBalancing	boolean		JDBC driver property: loadBalancing.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
longDataCacheSize	int Minimum: -1		JDBC driver property: longDataCacheSize.
netAddress	string		JDBC driver property: netAddress.
packetSize	int Minimum: -1 Maximum: 128		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
queryTimeout	A period of time with second precision		JDBC driver property: queryTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
resultsetMetaDataOptions	int		JDBC driver property: resultSetMetaDataOptions.
selectMethod	<ul style="list-style-type: none"> <li>• direct</li> <li>• cursor</li> </ul>		JDBC driver property: selectMethod.  <b>direct</b> direct <b>cursor</b> cursor
serverName	string	localhost	Server where the database is running.
snapshotSerializable	boolean		JDBC driver property: snapshotSerializable.

Attribute name	Data type	Default value	Description
spyAttributes	string		JDBC driver property: spyAttributes.
stringInputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringInputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
stringOutputParameterType	<ul style="list-style-type: none"> <li>varchar</li> <li>nvarchar</li> </ul>	varchar	JDBC driver property: stringOutputParameterType. <b>varchar</b> varchar <b>nvarchar</b> nvarchar
suppressConnectionWarnings	boolean		JDBC driver property: suppressConnectionWarnings.
transactionMode	<ul style="list-style-type: none"> <li>explicit</li> <li>implicit</li> </ul>		JDBC driver property: transactionMode. <b>explicit</b> explicit <b>implicit</b> implicit
truncateFractionalSeconds	boolean		JDBC driver property: truncateFractionalSeconds.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
useServerSideUpdatableCursors	boolean		JDBC driver property: useServerSideUpdatableCursors.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
validateServerCertificate	boolean		JDBC driver property: validateServerCertificate.

#### dataSource > properties.db2.i.native

Data source properties for the IBM DB2 for i Native JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>read only</li> <li>all</li> <li>read call</li> </ul>	all	JDBC driver property: access. <b>read only</b> read only <b>all</b> all <b>read call</b> read call

Attribute name	Data type	Default value	Description
autoCommit	boolean	true	JDBC driver property: autoCommit.
batchStyle	<ul style="list-style-type: none"> <li>• 2.1</li> <li>• 2.0</li> </ul>	2.0	JDBC driver property: batchStyle. <b>2.1</b> 2.1 <b>2.0</b> 2.0
behaviorOverride	int		JDBC driver property: behaviorOverride.
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive
dataTruncation	string	true	JDBC driver property: dataTruncation.
databaseName	string	*LOCAL	JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy
dateSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		JDBC driver property: dateSeparator. <b>\,</b> The comma character (,). <b>b</b> The character b <b>.</b> The period character (.). <b>/</b> The forward slash character (/). <b>-</b> The dash character (-).
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		JDBC driver property: decimalSeparator. <b>\,</b> The comma character (,). <b>.</b> The period character (.).
directMap	boolean	true	JDBC driver property: directMap.
doEscapeProcessing	boolean	true	JDBC driver property: doEscapeProcessing.
fullErrors	boolean		JDBC driver property: fullErrors.
libraries	string		JDBC driver property: libraries.
lobThreshold	int Maximum: 500000	0	JDBC driver property: lobThreshold.

Attribute name	Data type	Default value	Description
lockTimeout	A period of time with second precision	0	JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>• 31</li> <li>• 63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 63
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
networkProtocol	int		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.
prefetch	boolean	true	JDBC driver property: prefetch.
queryOptimizeGoal	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>	2	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).  <b>2</b> *ALLIO <b>1</b> *FIRSTIO

Attribute name	Data type	Default value	Description
reuseObjects	boolean	true	JDBC driver property: reuseObjects.
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
systemNaming	boolean	false	JDBC driver property: systemNaming.
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat.  <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• b</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  \, The comma character (,). <b>b</b> The character b : The colon character (:). . The period character (.).
trace	boolean		JDBC driver property: trace.
transactionTimeout	A period of time with second precision	0	JDBC driver property: transactionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateHex	<ul style="list-style-type: none"> <li>• binary</li> <li>• character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
useBlockInsert	boolean	false	JDBC driver property: useBlockInsert.

Attribute name	Data type	Default value	Description
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**dataSource > properties.db2.i.toolbox**

Data source properties for the IBM DB2 for i Toolbox JDBC driver.

false

Attribute name	Data type	Default value	Description
access	<ul style="list-style-type: none"> <li>• read only</li> <li>• all</li> <li>• read call</li> </ul>	all	JDBC driver property: access.  <b>read only</b> read only  <b>all</b> all  <b>read call</b> read call
behaviorOverride	int		JDBC driver property: behaviorOverride.
bidiImplicitReordering	boolean	true	JDBC driver property: bidiImplicitReordering.
bidiNumericOrdering	boolean	false	JDBC driver property: bidiNumericOrdering.
bidiStringType	int		JDBC driver property: bidiStringType.
bigDecimal	boolean	true	JDBC driver property: bigDecimal.
blockCriteria	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>	2	JDBC driver property: blockCriteria. Values are: 0 (no record blocking), 1 (block if FOR FETCH ONLY is specified), 2 (block if FOR UPDATE is specified).  <b>2</b> 2  <b>1</b> 1  <b>0</b> 0

Attribute name	Data type	Default value	Description
blockSize	<ul style="list-style-type: none"> <li>• 512</li> <li>• 128</li> <li>• 0</li> <li>• 32</li> <li>• 64</li> <li>• 16</li> <li>• 8</li> <li>• 256</li> </ul>	32	JDBC driver property: blockSize. <b>512</b> 512 <b>128</b> 128 <b>0</b> 0 <b>32</b> 32 <b>64</b> 64 <b>16</b> 16 <b>8</b> 8 <b>256</b> 256
cursorHold	boolean	false	JDBC driver property: cursorHold.
cursorSensitivity	<ul style="list-style-type: none"> <li>• asensitive</li> <li>• sensitive</li> <li>• insensitive</li> </ul>	asensitive	JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). <b>asensitive</b> asensitive <b>sensitive</b> sensitive <b>insensitive</b> insensitive
dataCompression	boolean	true	JDBC driver property: dataCompression.
dataTruncation	boolean	true	JDBC driver property: dataTruncation.
databaseName	string		JDBC driver property: databaseName.
dateFormat	<ul style="list-style-type: none"> <li>• dmy</li> <li>• iso</li> <li>• eur</li> <li>• ymd</li> <li>• julian</li> <li>• jis</li> <li>• usa</li> <li>• mdy</li> </ul>		JDBC driver property: dateFormat. <b>dmy</b> dmy <b>iso</b> iso <b>eur</b> eur <b>ymd</b> ymd <b>julian</b> julian <b>jis</b> jis <b>usa</b> usa <b>mdy</b> mdy

Attribute name	Data type	Default value	Description
dateSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• .</li> <li>• /</li> <li>• -</li> </ul>		<p>JDBC driver property: dateSeparator.</p> <p>The space character ( ).</p> <p>\, The comma character (,).</p> <p>. The period character (.</p> <p>/ The forward slash character (/).</p> <p>- The dash character (-).</p>
decimalSeparator	<ul style="list-style-type: none"> <li>• \,</li> <li>• .</li> </ul>		<p>JDBC driver property: decimalSeparator.</p> <p>\, The comma character (,).</p> <p>. The period character (.</p>
driver	<ul style="list-style-type: none"> <li>• toolbox</li> <li>• native</li> </ul>	toolbox	<p>JDBC driver property: driver.</p> <p><b>toolbox</b> toolbox</p> <p><b>native</b> native</p>
errors	<ul style="list-style-type: none"> <li>• full</li> <li>• basic</li> </ul>	basic	<p>JDBC driver property: errors.</p> <p><b>full</b> full</p> <p><b>basic</b> basic</p>
extendedDynamic	boolean	false	JDBC driver property: extendedDynamic.
extendedMetaData	boolean	false	JDBC driver property: extendedMetaData.
fullOpen	boolean	false	JDBC driver property: fullOpen.
holdInputLocators	boolean	true	JDBC driver property: holdInputLocators.
holdStatements	boolean	false	JDBC driver property: holdStatements.
isolationLevelSwitchingSupport	boolean	false	JDBC driver property: isolationLevelSwitchingSupport.
keepAlive	boolean		JDBC driver property: keepAlive.
lazyClose	boolean	false	JDBC driver property: lazyClose.
libraries	string		JDBC driver property: libraries.

Attribute name	Data type	Default value	Description
lobThreshold	int Minimum: 0 Maximum: 16777216	0	JDBC driver property: lobThreshold.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
maximumPrecision	<ul style="list-style-type: none"> <li>• 31</li> <li>• 63</li> </ul>	31	JDBC driver property: maximumPrecision.  <b>31</b> 31 <b>63</b> 64
maximumScale	int Minimum: 0 Maximum: 63	31	JDBC driver property: maximumScale.
metaDataSource	int Minimum: 0 Maximum: 1	1	JDBC driver property: metaDataSource.
minimumDivideScale	int Minimum: 0 Maximum: 9	0	JDBC driver property: minimumDivideScale.
naming	<ul style="list-style-type: none"> <li>• system</li> <li>• sql</li> </ul>	sql	JDBC driver property: naming.  <b>system</b> system <b>sql</b> sql
package	string		JDBC driver property: package.
packageAdd	boolean	true	JDBC driver property: packageAdd.
packageCCSID	<ul style="list-style-type: none"> <li>• 13488</li> <li>• 1200</li> </ul>	13488	JDBC driver property: packageCCSID. Values are: 1200 (UCS-2) or 13488 (UTF-16).  <b>13488</b> 13488 (UTF-16) <b>1200</b> 1200 (UCS-2)
packageCache	boolean	false	JDBC driver property: packageCache.

Attribute name	Data type	Default value	Description
packageCriteria	<ul style="list-style-type: none"> <li>default</li> <li>select</li> </ul>	default	JDBC driver property: packageCriteria. <b>default</b> default <b>select</b> select
packageError	<ul style="list-style-type: none"> <li>exception</li> <li>none</li> <li>warning</li> </ul>	warning	JDBC driver property: packageError. <b>exception</b> exception <b>none</b> none <b>warning</b> warning
packageLibrary	string	QGPL	JDBC driver property: packageLibrary.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
prefetch	boolean	true	JDBC driver property: prefetch.
prompt	boolean	false	JDBC driver property: prompt.
proxyServer	string		JDBC driver property: proxyServer.
qaqqiniLibrary	string		JDBC driver property: qaqqiniLibrary.
queryOptimizeGoal	int Minimum: 0 Maximum: 2	0	JDBC driver property: queryOptimizeGoal. Values are: 1 (*FIRSTIO) or 2 (*ALLIO).
receiveBufferSize	int Minimum: 1		JDBC driver property: receiveBufferSize.
remarks	<ul style="list-style-type: none"> <li>system</li> <li>sql</li> </ul>	system	JDBC driver property: remarks. <b>system</b> system <b>sql</b> sql
rollbackCursorHold	boolean	false	JDBC driver property: rollbackCursorHold.
savePasswordWhenSerialized	boolean	false	JDBC driver property: savePasswordWhenSerialized.
secondaryUrl	string		JDBC driver property: secondaryUrl.
secure	boolean	false	JDBC driver property: secure.
sendBufferSize	int Minimum: 1		JDBC driver property: sendBufferSize.

Attribute name	Data type	Default value	Description
serverName	string		Server where the database is running.
serverTraceCategories	int	0	JDBC driver property: serverTraceCategories.
soLinger	A period of time with second precision		JDBC driver property: soLinger. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
soTimeout	A period of time with millisecond precision		JDBC driver property: soTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
sort	<ul style="list-style-type: none"> <li>• hex</li> <li>• table</li> <li>• language</li> </ul>	hex	JDBC driver property: sort. <b>hex</b> hex <b>table</b> table <b>language</b> language
sortLanguage	string		JDBC driver property: sortLanguage.
sortTable	string		JDBC driver property: sortTable.
sortWeight	<ul style="list-style-type: none"> <li>• unqiue</li> <li>• shared</li> </ul>		JDBC driver property: sortWeight. <b>unqiue</b> unique <b>shared</b> shared
tcpNoDelay	boolean		JDBC driver property: tcpNoDelay.
threadUsed	boolean	true	JDBC driver property: threadUsed.

Attribute name	Data type	Default value	Description
timeFormat	<ul style="list-style-type: none"> <li>• iso</li> <li>• eur</li> <li>• jis</li> <li>• usa</li> <li>• hms</li> </ul>		JDBC driver property: timeFormat. <b>iso</b> iso <b>eur</b> eur <b>jis</b> jis <b>usa</b> usa <b>hms</b> hms
timeSeparator	<ul style="list-style-type: none"> <li>•</li> <li>• \,</li> <li>• :</li> <li>• .</li> </ul>		JDBC driver property: timeSeparator.  The space character ( ). \, The comma character (,). : The colon character (:). . The period character (.).
toolboxTrace	<ul style="list-style-type: none"> <li>• diagnostic</li> <li>• information</li> <li>• conversion</li> <li>• error</li> <li>• thread</li> <li>• proxy</li> <li>• none</li> <li>• datastream</li> <li>• pcml</li> <li>• all</li> <li>• jdbc</li> <li>• warning</li> </ul>		JDBC driver property: toolboxTrace. <b>diagnostic</b> diagnostic <b>information</b> information <b>conversion</b> conversion <b>error</b> error <b>thread</b> thread <b>proxy</b> proxy <b>none</b> none <b>datastream</b> datastream <b>pcml</b> pcml <b>all</b> all <b>jdbc</b> jdbc <b>warning</b> warning
trace	boolean		JDBC driver property: trace.
translateBinary	boolean	false	JDBC driver property: translateBinary.
translateBoolean	boolean	true	JDBC driver property: translateBoolean.

Attribute name	Data type	Default value	Description
translateHex	<ul style="list-style-type: none"> <li>binary</li> <li>character</li> </ul>	character	JDBC driver property: translateHex.  <b>binary</b> binary <b>character</b> character
trueAutoCommit	boolean	false	JDBC driver property: trueAutoCommit.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaLooselyCoupledSupport	int  Minimum: 0  Maximum: 1	0	JDBC driver property: xaLooselyCoupledSupport.

#### dataSource > properties.db2.jcc

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for DB2.

false

Attribute name	Data type	Default value	Description
activateDatabase	int		JDBC driver property: activateDatabase.
alternateGroupDatabaseName	string		JDBC driver property: alternateGroupDatabaseName.
alternateGroupPortNumber	string		JDBC driver property: alternateGroupPortNumber.
alternateGroupServerName	string		JDBC driver property: alternateGroupServerName.
blockingReadConnectionTimeout	A period of time with second precision		JDBC driver property: blockingReadConnectionTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
clientAccountingInformation	string		JDBC driver property: clientAccountingInformation.
clientApplicationInformation	string		JDBC driver property: clientApplicationInformation.
clientRerouteAlternatePortNumber	string		JDBC driver property: clientRerouteAlternatePortNumber.
clientRerouteAlternateServerName	string		JDBC driver property: clientRerouteAlternateServerName.

Attribute name	Data type	Default value	Description
clientUser	string		JDBC driver property: clientUser.
clientWorkstation	string		JDBC driver property: clientWorkstation.
connectionCloseWithInFlightTransaction	Transaction • 1		JDBC driver property: connectionCloseWithInFlightTransaction. 2 CONNECTION_CLOSE_WITH_ROLLBACK 1 CONNECTION_CLOSE_WITH_EXCEPTION
currentAlternateGroupEntry	int		JDBC driver property: currentAlternateGroupEntry.
currentFunctionPath	string		JDBC driver property: currentFunctionPath.
currentLocaleLcCtype	string		JDBC driver property: currentLocaleLcCtype.
currentLockTimeout	A period of time with second precision		JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
currentPackagePath	string		JDBC driver property: currentPackagePath.
currentPackageSet	string		JDBC driver property: currentPackageSet.
currentSQLID	string		JDBC driver property: currentSQLID.
currentSchema	string		JDBC driver property: currentSchema.
cursorSensitivity	• 2 • 1 • 0		JDBC driver property: cursorSensitivity. Values are: 0 (TYPE_SCROLL_SENSITIVE_STATIC), 1 (TYPE_SCROLL_SENSITIVE_DYNAMIC), 2 (TYPE_SCROLL_ASENSITIVE). 2 TYPE_SCROLL_ASENSITIVE 1 TYPE_SCROLL_SENSITIVE_DYNAMIC 0 TYPE_SCROLL_SENSITIVE_STATIC
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean	true	JDBC driver property: deferPrepares.

Attribute name	Data type	Default value	Description
driverType	<ul style="list-style-type: none"> <li>2</li> <li>4</li> </ul>	4	JDBC driver property: driverType. 2 Type 2 JDBC driver. 4 Type 4 JDBC driver.
enableAlternateGroupSeamlessACR	boolean		JDBC driver property: enableAlternateGroupSeamlessACR.
enableClientAffinitiesList	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableClientAffinitiesList. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableExtendedDescribe	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedDescribe. 2 NO 1 YES
enableExtendedIndicators	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableExtendedIndicators. 2 NO 1 YES
enableNamedParameterMarkers	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSeamlessFailover	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeInputStreams	boolean		JDBC driver property: fullyMaterializeInputStreams.
fullyMaterializeInputStreamsOnBatchExecution	<ul style="list-style-type: none"> <li>1</li> </ul>		JDBC driver property: fullyMaterializeInputStreamsOnBatchExecution. 2 NO 1 YES
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.

Attribute name	Data type	Default value	Description
implicitRollbackOption	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: implicitRollbackOption.</p> <p>2 IMPLICIT_ROLLBACK_OPTION_CLOSE</p> <p>1 IMPLICIT_ROLLBACK_OPTION_NO</p> <p>0 IMPLICIT_ROLLBACK_OPTION_NO</p>
interruptProcessingMode	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• 0</li> </ul>		<p>JDBC driver property: interruptProcessingMode.</p> <p>2 INTERRUPT_PROCESSING_MODE_C</p> <p>1 INTERRUPT_PROCESSING_MODE_S</p> <p>0 INTERRUPT_PROCESSING_MODE_D</p>
keepAliveTimeOut	A period of time with second precision		<p>JDBC driver property: keepAliveTimeOut. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
keepDynamic	int		JDBC driver property: keepDynamic.
kerberosServerPrincipal	string		JDBC driver property: kerberosServerPrincipal.
loginTimeout	A period of time with second precision		<p>JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.</p>
maxConnCachedParamBufferSize	int		JDBC driver property: maxConnCachedParamBufferSize.
maxRetriesForClientReroute	int		JDBC driver property: maxRetriesForClientReroute.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	50000	Port on which to obtain database connections.
profileName	string		JDBC driver property: profileName.

Attribute name	Data type	Default value	Description
queryCloseImplicit	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: queryCloseImplicit. Values are: 1 (QUERY_CLOSE_IMPLICIT_YES) or 2 (QUERY_CLOSE_IMPLICIT_NO).</p> <p>2        QUERY_CLOSE_IMPLICIT_NO 1        QUERY_CLOSE_IMPLICIT_YES</p>
queryDataSize	<p>int</p> <p>Minimum: 4096</p> <p>Maximum: 65535</p>		JDBC driver property: queryDataSize.
queryTimeoutInterruptProcessingMode	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: queryTimeoutInterruptProcessingMode.</p> <p>2        INTERRUPT_PROCESSING_MODAL 1        INTERRUPT_PROCESSING_MODAL</p>
readOnly	boolean		JDBC driver property: readOnly.
recordTemporalHistory	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: recordTemporalHistory.</p> <p>2        NO 1        YES</p>
resultSetHoldability	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2        CLOSE_CURSORS_AT_COMMIT 1        HOLD_CURSORS_OVER_COMMIT</p>
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2        CLOSE_CURSORS_AT_COMMIT 1        HOLD_CURSORS_OVER_COMMIT</p>
retrieveMessagesFromServerOnGetMessage	boolean	true	JDBC driver property: retrieveMessagesFromServerOnGetMessage.

Attribute name	Data type	Default value	Description
retryIntervalForClientReroute	A period of time with second precision		JDBC driver property: retryIntervalForClientReroute. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 18</li> <li>• 15</li> <li>• 9</li> <li>• 16</li> <li>• 13</li> <li>• 11</li> <li>• 12</li> </ul>		<p>JDBC driver property: securityMechanism. Values are:</p> <ul style="list-style-type: none"> <li>3 (CLEAR_TEXT_PASSWORD_SECURITY),</li> <li>4 (USER_ONLY_SECURITY),</li> <li>7 (ENCRYPTED_PASSWORD_SECURITY),</li> <li>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY),</li> <li>11 (KERBEROS_SECURITY),</li> <li>12 (ENCRYPTED_USER_AND_DATA_SECURITY),</li> <li>13 (ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY),</li> <li>15 (PLUGIN_SECURITY),</li> <li>16 (ENCRYPTED_USER_ONLY_SECURITY),</li> <li>18 (TLS_CLIENT_CERTIFICATE_SECURITY).</li> </ul> <p>3 CLEAR_TEXT_PASSWORD_SECURITY  7 ENCRYPTED_PASSWORD_SECURITY  4 USER_ONLY_SECURITY  18 TLS_CLIENT_CERTIFICATE_SECURITY  15 PLUGIN_SECURITY  9 ENCRYPTED_USER_AND_PASSWORD_SECURITY  16 ENCRYPTED_USER_ONLY_SECURITY  13 ENCRYPTED_USER_PASSWORD_AND_DATA_SECURITY  11 KERBEROS_SECURITY  12 ENCRYPTED_USER_AND_DATA_SECURITY</p>
sendDataAsIs	boolean		JDBC driver property: sendDataAsIs.
serverName	string	localhost	Server where the database is running.
sessionTimeZone	string		JDBC driver property: sessionTimeZone.
sqljCloseStmtsWithOpenResultSet	boolean		JDBC driver property: sqljCloseStmtsWithOpenResultSet.

Attribute name	Data type	Default value	Description
sqljEnableClassLoaderSpecificProfiles	boolean		JDBC driver property: sqljEnableClassLoaderSpecificProfiles.
sslConnection	boolean		JDBC driver property: sslConnection.
streamBufferSize	int		JDBC driver property: streamBufferSize.
stripTrailingZerosForDecimalNumbers	Numbers <ul style="list-style-type: none"> <li>• 1</li> </ul>		JDBC driver property: stripTrailingZerosForDecimalNumbers. 2 NO 1 YES
sysSchema	string		JDBC driver property: sysSchema.
timerLevelForQueryTimeOut	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> <li>• -1</li> </ul>		JDBC driver property: timerLevelForQueryTimeOut. 2 QUERYTIMEOUT_CONNECTION 1 QUERYTIMEOUT_STATEMENT_L -1 QUERYTIMEOUT_DISABLED
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceFileCount	int		JDBC driver property: traceFileCount.
traceFileSize	int		JDBC driver property: traceFileSize.
traceLevel	int	0	Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
traceOption	<ul style="list-style-type: none"> <li>• 1</li> <li>• 0</li> </ul>		JDBC driver property: traceOption 1 1 0 0

Attribute name	Data type	Default value	Description
translateForBitData	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: translateForBitData. 2 SERVER_ENCODING_REPRESENTATION 1 HEX_REPRESENTATION
updateCountForBatch	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: updateCountForBatch. 2 TOTAL_UPDATE_COUNT 1 NO_UPDATE_COUNT
useCachedCursor	boolean		JDBC driver property: useCachedCursor.
useIdentityValLocalForAutoGeneratedKeys	boolean		JDBC driver property: useIdentityValLocalForAutoGeneratedKeys.
useJDBC41DefinitionForGetColumns	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC41DefinitionForGetColumns. 2 NO 1 YES
useJDBC4ColumnNameAndLabelSemantics	<ul style="list-style-type: none"> <li>2</li> <li>1</li> </ul>		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO). 2 NO 1 YES
useTransactionRedirect	boolean		JDBC driver property: useTransactionRedirect.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
xaNetworkOptimization	boolean		JDBC driver property: xaNetworkOptimization.

**dataSource > properties.derby.client**

Data source properties for Derby Network Client JDBC driver.

false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1527	Port on which to obtain database connections.
retrieveMessageText	boolean	true	JDBC driver property: retrieveMessageText.
securityMechanism	<ul style="list-style-type: none"> <li>3</li> <li>7</li> <li>4</li> <li>9</li> <li>8</li> </ul>	3	<p>JDBC driver property: securityMechanism. Values are:</p> <p>3 (CLEAR_TEXT_PASSWORD_SECURITY),</p> <p>4 (USER_ONLY_SECURITY),</p> <p>7 (ENCRYPTED_PASSWORD_SECURITY),</p> <p>8 (STRONG_PASSWORD_SUBSTITUTE_SECURITY),</p> <p>9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY)</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY</p> <p>7 ENCRYPTED_PASSWORD_SECURITY</p> <p>4 USER_ONLY_SECURITY</p> <p>9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p> <p>8 STRONG_PASSWORD_SUBSTITUTE_SECURITY</p>

Attribute name	Data type	Default value	Description
serverName	string	localhost	Server where the database is running.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		JDBC driver property: shutdownDatabase. <b>false</b> Do not shut down the database. <b>shutdown</b> Shut down the database when a connection is attempted.
ssl	<ul style="list-style-type: none"> <li>basic</li> <li>off</li> <li>peerAuthentication</li> </ul>		JDBC driver property: ssl. <b>basic</b> basic <b>off</b> off <b>peerAuthentication</b> peerAuthentication
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_XA_CALLS=2048, TRACE_ALL=-1.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**dataSource > properties.derby.embedded**

Data source properties for Derby Embedded JDBC driver.

false

Attribute name	Data type	Default value	Description
connectionAttributes	string		JDBC driver property: connectionAttributes.

Attribute name	Data type	Default value	Description
createDatabase	<ul style="list-style-type: none"> <li>false</li> <li>create</li> </ul>		<p>JDBC driver property: createDatabase.</p> <p><b>false</b> Do not automatically create the database.</p> <p><b>create</b> When the first connection is established, automatically create the database if it doesn't exist.</p>
databaseName	string		JDBC driver property: databaseName.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
shutdownDatabase	<ul style="list-style-type: none"> <li>false</li> <li>shutdown</li> </ul>		<p>JDBC driver property: shutdownDatabase.</p> <p><b>false</b> Do not shut down the database.</p> <p><b>shutdown</b> Shut down the database when a connection is attempted.</p>
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

#### dataSource > properties.informix

Data source properties for the Informix JDBC driver.

false

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
ifxCLIENT_LOCALE	string		JDBC driver property: ifxCLIENT_LOCALE.
ifxCPMAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMInitPoolSize	int		JDBC driver property: ifxCPMInitPoolSize.
ifxCPMMaxConnections	int		JDBC driver property: ifxCPMMaxConnections.
ifxCPMMaxPoolSize	int		JDBC driver property: ifxCPMMaxPoolSize.
ifxCPMMinAgeLimit	A period of time with second precision		JDBC driver property: ifxCPMMinAgeLimit. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxCPMMinPoolSize	int		JDBC driver property: ifxCPMMinPoolSize.
ifxCPMServiceInterval	A period of time with millisecond precision		JDBC driver property: ifxCPMServiceInterval. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxDBANSIWARN	boolean		JDBC driver property: ifxDBANSIWARN.
ifxDBCENTURY	string		JDBC driver property: ifxDBCENTURY.
ifxDBDATE	string		JDBC driver property: ifxDBDATE.
ifxDBSPACETEMP	string		JDBC driver property: ifxDBSPACETEMP.

Attribute name	Data type	Default value	Description
ifxDBTEMP	string		JDBC driver property: ifxDBTEMP.
ifxDBTIME	string		JDBC driver property: ifxDBTIME.
ifxDBUPSPACE	string		JDBC driver property: ifxDBUPSPACE.
ifxDB_LOCALE	string		JDBC driver property: ifxDB_LOCALE.
ifxDELIMIDENT	boolean		JDBC driver property: ifxDELIMIDENT.
ifxENABLE_TYPE_CACHE	boolean		JDBC driver property: ifxENABLE_TYPE_CACHE.
ifxFET_BUF_SIZE	int		JDBC driver property: ifxFET_BUF_SIZE.
ifxGL_DATE	string		JDBC driver property: ifxGL_DATE.
ifxGL_DATETIME	string		JDBC driver property: ifxGL_DATETIME.
ifxIFXHOST	string	localhost	JDBC driver property: ifxIFXHOST.
ifxIFX_AUTOFREE	boolean		JDBC driver property: ifxIFX_AUTOFREE.
ifxIFX_DIRECTIVES	string		JDBC driver property: ifxIFX_DIRECTIVES.
ifxIFX_LOCK_MODE_WAIT	A period of time with second precision	2s	JDBC driver property: ifxIFX_LOCK_MODE_WAIT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxIFX_SOC_TIMEOUT	A period of time with millisecond precision		JDBC driver property: ifxIFX_SOC_TIMEOUT. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
ifxIFX_USEPUT	boolean		JDBC driver property: ifxIFX_USEPUT.

Attribute name	Data type	Default value	Description
ifxIFX_USE_STRENC	boolean		JDBC driver property: ifxIFX_USE_STRENC.
ifxIFX_XASPEC	string	y	JDBC driver property: ifxIFX_XASPEC.
ifxINFORMIXCONRETRY	int		JDBC driver property: ifxINFORMIXCONRETRY.
ifxINFORMIXCONTIME	A period of time with second precision		JDBC driver property: ifxINFORMIXCONTIME. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
ifxINFORMIXOPCACHE	string		JDBC driver property: ifxINFORMIXOPCACHE.
ifxINFORMIXSTACKSIZE	int		JDBC driver property: ifxINFORMIXSTACKSIZE.
ifxJDBCTEMP	string		JDBC driver property: ifxJDBCTEMP.
ifxLDAP_IFXBASE	string		JDBC driver property: ifxLDAP_IFXBASE.
ifxLDAP_PASSWD	string		JDBC driver property: ifxLDAP_PASSWD.
ifxLDAP_URL	string		JDBC driver property: ifxLDAP_URL.
ifxLDAP_USER	string		JDBC driver property: ifxLDAP_USER.
ifxLOBCACHE	int		JDBC driver property: ifxLOBCACHE.
ifxNEWCODESET	string		JDBC driver property: ifxNEWCODESET.
ifxNEWLOCALE	string		JDBC driver property: ifxNEWLOCALE.
ifxNODEFDAC	string		JDBC driver property: ifxNODEFDAC.
ifxOPTCOMPIND	string		JDBC driver property: ifxOPTCOMPIND.
ifxOPTOFC	string		JDBC driver property: ifxOPTOFC.
ifxOPT_GOAL	string		JDBC driver property: ifxOPT_GOAL.
ifxPATH	string		JDBC driver property: ifxPATH.
ifxPDQPRIORITY	string		JDBC driver property: ifxPDQPRIORITY.

Attribute name	Data type	Default value	Description
ifxPLCONFIG	string		JDBC driver property: ifxPLCONFIG.
ifxPLOAD_LO_PATH	string		JDBC driver property: ifxPLOAD_LO_PATH.
ifxPROTOCOLTRACE	int		JDBC driver property: ifxPROTOCOLTRACE.
ifxPROTOCOLTRACEFILE	string		JDBC driver property: ifxPROTOCOLTRACEFILE.
ifxPROXY	string		JDBC driver property: ifxPROXY.
ifxPSORT_DBTEMP	string		JDBC driver property: ifxPSORT_DBTEMP.
ifxPSORT_NPROCS	boolean		JDBC driver property: ifxPSORT_NPROCS.
ifxSECURITY	string		JDBC driver property: ifxSECURITY.
ifxSQLH_FILE	string		JDBC driver property: ifxSQLH_FILE.
ifxSQLH_LOC	string		JDBC driver property: ifxSQLH_LOC.
ifxSQLH_TYPE	string		JDBC driver property: ifxSQLH_TYPE.
ifxSSLCONNECTION	string		JDBC driver property: ifxSSLCONNECTION.
ifxSTMT_CACHE	string		JDBC driver property: ifxSTMT_CACHE.
ifxTRACE	int		JDBC driver property: ifxTRACE.
ifxTRACEFILE	string		JDBC driver property: ifxTRACEFILE.
ifxTRUSTED_CONTEXT	string		JDBC driver property: ifxTRUSTED_CONTEXT.
ifxUSEV5SERVER	boolean		JDBC driver property: ifxUSEV5SERVER.
ifxUSE_DTENV	boolean		JDBC driver property: ifxUSE_DTENV.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
roleName	string		JDBC driver property: roleName.
serverName	string		Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

**dataSource > properties.informix.jcc**

Data source properties for the IBM Data Server Driver for JDBC and SQLJ for Informix.

false

Attribute name	Data type	Default value	Description
DBANSIWARN	boolean		JDBC driver property: DBANSIWARN.
DBDATE	string		JDBC driver property: DBDATE.
DBPATH	string		JDBC driver property: DBPATH.
DBSPACETEMP	string		JDBC driver property: DBSPACETEMP.
DBTEMP	string		JDBC driver property: DBTEMP.
DBUPSPACE	string		JDBC driver property: DBUPSPACE.
DELIMIDENT	boolean		JDBC driver property: DELIMIDENT.
IFX_DIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_DIRECTIVES. <b>ON</b> ON <b>OFF</b> OFF
IFX_EXTDIRECTIVES	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>		JDBC driver property: IFX_EXTDIRECTIVES. <b>ON</b> ON <b>OFF</b> OFF
IFX_UPDESC	string		JDBC driver property: IFX_UPDESC.

Attribute name	Data type	Default value	Description
IFX_XASTDCOMPLIANCE_XAEND	<ul style="list-style-type: none"> <li>0</li> </ul>		JDBC driver property: IFX_XASTDCOMPLIANCE_XAEND. <b>1</b> 1 <b>0</b> 0
INFORMIXOPCACHE	string		JDBC driver property: INFORMIXOPCACHE.
INFORMIXSTACKSIZE	string		JDBC driver property: INFORMIXSTACKSIZE.
NODEFDAC	<ul style="list-style-type: none"> <li>yes</li> <li>no</li> </ul>		JDBC driver property: NODEFDAC. <b>yes</b> yes <b>no</b> no
OPTCOMPIND	<ul style="list-style-type: none"> <li>2</li> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTCOMPIND. <b>2</b> 2 <b>1</b> 1 <b>0</b> 0
OPTOFC	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: OPTOFC. <b>1</b> 1 <b>0</b> 0
PDQPRIORITY	<ul style="list-style-type: none"> <li>HIGH</li> <li>LOW</li> <li>OFF</li> </ul>		JDBC driver property: PDQPRIORITY. <b>HIGH</b> HIGH <b>LOW</b> LOW <b>OFF</b> OFF
PSORT_DBTEMP	string		JDBC driver property: PSORT_DBTEMP.
PSORT_NPROCS	string Maximum: 10		JDBC driver property: PSORT_NPROCS.
STMT_CACHE	<ul style="list-style-type: none"> <li>1</li> <li>0</li> </ul>		JDBC driver property: STMT_CACHE. <b>1</b> 1 <b>0</b> 0
currentLockTimeout	A period of time with second precision	2s	JDBC driver property: currentLockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
deferPrepares	boolean		JDBC driver property: deferPrepares.
driverType	int	4	JDBC driver property: driverType.
enableNamedParameterMarkers	int		JDBC driver property: enableNamedParameterMarkers. Values are: 1 (YES) or 2 (NO).
enableSeamlessFailover	int		JDBC driver property: enableSeamlessFailover. Values are: 1 (YES) or 2 (NO).
enableSysplexWLB	boolean		JDBC driver property: enableSysplexWLB.
fetchSize	int		JDBC driver property: fetchSize.
fullyMaterializeLobData	boolean		JDBC driver property: fullyMaterializeLobData.
keepDynamic	int		JDBC driver property: keepDynamic.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1526	Port on which to obtain database connections.
progressiveStreaming	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		JDBC driver property: progressiveStreaming. Values are: 1 (YES) or 2 (NO).  2 NO 1 YES
queryDataSize	int  Minimum: 4096  Maximum: 10485760		JDBC driver property: queryDataSize.

Attribute name	Data type	Default value	Description
resultSetHoldability	<ul style="list-style-type: none"> <li>• 2</li> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldability. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
resultSetHoldabilityForCatalogQueries	<ul style="list-style-type: none"> <li>• 1</li> </ul>		<p>JDBC driver property: resultSetHoldabilityForCatalogQueries. Values are: 1 (HOLD_CURSORS_OVER_COMMIT) or 2 (CLOSE_CURSORS_AT_COMMIT).</p> <p>2 CLOSE_CURSORS_AT_COMMIT 1 HOLD_CURSORS_OVER_COMMIT</p>
retrieveMessagesFromServerOnGetMessage	boolean	true	<p>JDBC driver property: retrieveMessagesFromServerOnGetMessage.</p>
securityMechanism	<ul style="list-style-type: none"> <li>• 3</li> <li>• 7</li> <li>• 4</li> <li>• 9</li> </ul>		<p>JDBC driver property: securityMechanism. Values are: 3 (CLEAR_TEXT_PASSWORD_SECURITY), 4 (USER_ONLY_SECURITY), 7 (ENCRYPTED_PASSWORD_SECURITY), 9 (ENCRYPTED_USER_AND_PASSWORD_SECURITY).</p> <p>3 CLEAR_TEXT_PASSWORD_SECURITY 7 ENCRYPTED_PASSWORD_SECURITY 4 USER_ONLY_SECURITY 9 ENCRYPTED_USER_AND_PASSWORD_SECURITY</p>
serverName	string	localhost	Server where the database is running.
traceDirectory	string		JDBC driver property: traceDirectory.
traceFile	string		JDBC driver property: traceFile.
traceFileAppend	boolean		JDBC driver property: traceFileAppend.

Attribute name	Data type	Default value	Description
traceLevel	int		Bitwise combination of the following constant values: TRACE_NONE=0, TRACE_CONNECTION_CALLS=1, TRACE_STATEMENT_CALLS=2, TRACE_RESULT_SET_CALLS=4, TRACE_DRIVER_CONFIGURATION=16, TRACE_CONNECTS=32, TRACE_DRDA_FLOWS=64, TRACE_RESULT_SET_META_DATA=128, TRACE_PARAMETER_META_DATA=256, TRACE_DIAGNOSTICS=512, TRACE_SQLJ=1024, TRACE_META_CALLS=8192, TRACE_DATASOURCE_CALLS=16384, TRACE_LARGE_OBJECT_CALLS=32768, TRACE_SYSTEM_MONITOR=131072, TRACE_TRACEPOINTS=262144, TRACE_ALL=-1.
useJDBC4ColumnNameAndLabelSemantics	int		JDBC driver property: useJDBC4ColumnNameAndLabelSemantics. Values are: 1 (YES) or 2 (NO).
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

#### dataSource > properties.microsoft.sqlserver

Data source properties for Microsoft SQL Server JDBC Driver.

false

Attribute name	Data type	Default value	Description
URL	string		URL for connecting to the database. Example: jdbc:sqlserver://localhost:1433;databaseName=myDB.
applicationIntent	<ul style="list-style-type: none"> <li>ReadOnly</li> <li>ReadWrite</li> </ul>		JDBC driver property: applicationIntent. <b>ReadOnly</b> ReadOnly <b>ReadWrite</b> ReadWrite
applicationName	string		JDBC driver property: applicationName.
authenticationScheme	<ul style="list-style-type: none"> <li>NativeAuthentication</li> <li>JavaKerberos</li> </ul>		JDBC driver property: authenticationScheme. <b>NativeAuthentication</b> NativeAuthentication <b>JavaKerberos</b> JavaKerberos

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
encrypt	boolean		JDBC driver property: encrypt.
failoverPartner	string		JDBC driver property: failoverPartner.
hostNameInCertificate	string		JDBC driver property: hostNameInCertificate.
instanceName	string		JDBC driver property: instanceName.
integratedSecurity	boolean		JDBC driver property: integratedSecurity.
lastUpdateCount	boolean		JDBC driver property: lastUpdateCount.
lockTimeout	A period of time with millisecond precision		JDBC driver property: lockTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
multiSubnetFailover	boolean		JDBC driver property: multiSubnetFailover.
packetSize	int Minimum: 512 Maximum: 32767		JDBC driver property: packetSize.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int		Port on which to obtain database connections.

Attribute name	Data type	Default value	Description
responseBuffering	<ul style="list-style-type: none"> <li>full</li> <li>adaptive</li> </ul>		JDBC driver property: responseBuffering. <b>full</b> full <b>adaptive</b> adaptive
selectMethod	<ul style="list-style-type: none"> <li>direct</li> <li>cursor</li> </ul>		JDBC driver property: selectMethod. <b>direct</b> direct <b>cursor</b> cursor
sendStringParametersAsUnicode	boolean	false	JDBC driver property: sendStringParametersAsUnicode.
sendTimeAsDatetime	boolean		JDBC driver property: sendTimeAsDatetime.
serverName	string	localhost	Server where the database is running.
trustServerCertificate	boolean		JDBC driver property: trustServerCertificate.
trustStore	string		JDBC driver property: trustStore.
trustStorePassword	Reversably encoded password (string)		JDBC driver property: trustStorePassword.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
workstationID	string		JDBC driver property: workstationID.
xopenStates	boolean		JDBC driver property: xopenStates.

#### dataSource > properties.oracle

Data source properties for Oracle JDBC driver.

false

Attribute name	Data type	Default value	Description
ONSConfiguration	string		JDBC driver property: ONSConfiguration.
TNSEntryName	string		JDBC driver property: TNSEntryName.
URL	string		URL for connecting to the database. Examples: jdbc:oracle:thin:@//localhost:1521/sample or jdbc:oracle:oci:@//localhost:1521/sample.
connectionProperties	string		JDBC driver property: connectionProperties.

Attribute name	Data type	Default value	Description
databaseName	string		JDBC driver property: databaseName.
driverType	<ul style="list-style-type: none"> <li>oci</li> <li>thin</li> </ul>	thin	JDBC driver property: driverType.  <b>oci</b> oci <b>thin</b> thin
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	string		JDBC driver property: networkProtocol.
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	1521	Port on which to obtain database connections.
serverName	string	localhost	Server where the database is running.
serviceName	string		JDBC driver property: serviceName.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.

#### dataSource > properties.sybase

Data source properties for Sybase JDBC driver.

false

Attribute name	Data type	Default value	Description
SERVER_INITIATED_TRANSACTIONS	<ul style="list-style-type: none"> <li>false</li> <li>true</li> </ul>	false	JDBC driver property: SERVER_INITIATED_TRANSACTIONS.  <b>false</b> false <b>true</b> true
connectionProperties	string	SELECT_OPENS_CURSOR=true	JDBC driver property: connectionProperties.
databaseName	string		JDBC driver property: databaseName.

Attribute name	Data type	Default value	Description
loginTimeout	A period of time with second precision		JDBC driver property: loginTimeout. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
networkProtocol	<ul style="list-style-type: none"> <li>• SSL</li> <li>• socket</li> </ul>		JDBC driver property: networkProtocol.  <b>SSL</b> SSL <b>socket</b> socket
password	Reversably encoded password (string)		It is recommended to use a container managed authentication alias instead of configuring this property.
portNumber	int	5000	Port on which to obtain database connections.
resourceManagerName	string		JDBC driver property: resourceManagerName.
serverName	string	localhost	Server where the database is running.
user	string		It is recommended to use a container managed authentication alias instead of configuring this property.
version	int		JDBC driver property: version.

**dataSource > recoveryAuthData**

Authentication data for transaction recovery.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user to use when connecting to the EIS. The value can be stored in clear text or encoded form. It is recommended that you encode the password. To do so, use the securityUtility tool with the encode option.
user	string		Name of the user to use when connecting to the EIS.

## Trust Association Interceptor (trustAssociation)

Controls the operation of the trust association interceptor (TAI).

- interceptors
  - library
    - file
    - fileset
    - folder
  - properties

Attribute name	Data type	Default value	Description
failOverToAppAuthType	boolean	false	Allow an interceptor to fall back to the application authentication mechanism.
id	string		A unique configuration ID.
invokeForUnprotectedURI	boolean	false	Controls whether the TAI is invoked for an unprotected URI.

### interceptors

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
className	string		Fully-qualified package name of the interceptor class.
enabled	boolean	true	Enables or disables the interceptor.
id	string		A unique configuration ID.
invokeAfterSSO	boolean	true	Invoke an interceptor after single sign-on (SSO).
invokeBeforeSSO	boolean	false	Invoke an interceptor before single sign-on (SSO).
libraryRef	A reference to top level library element (string).		A reference to the ID of the shared library configuration.

### interceptors > library

A reference to the ID of the shared library configuration.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.

Attribute name	Data type	Default value	Description
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
name	string		Name of shared library for administrators

**interceptors > library > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**interceptors > library > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

#### interceptors > library > folder

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

#### interceptors > properties

Collection of properties for the interceptor.

false

## User Information (userInfo)

Specifies the user information that is included in the response of the openID provider.

Attribute name	Data type	Default value	Description
alias	string	email	Specifies an alias name.
count	int Minimum: 1	1	Specifies how much userInfo is included in the response of the openID provider.
id	string		A unique configuration ID.
required	boolean	true	Specifies whether user information is required or not.
uriType	string	http://axschema.org/contact/email	Specifies a URI type.

## Variable Declaration (variable)

Declare a new variable by specifying the name and value for the variable.

Attribute name	Data type	Default value	Description
name	string		The name of the variable.
value	string		The value to be assigned to the variable.

## Virtual Host (virtualHost)

A virtual host provides a logical grouping for configuring web applications to a particular host name. The default virtual host (default\_host) is suitable for most simple configurations.

- allowFromEndpoint
  - accessLogging
  - httpOptions
  - sslOptions
  - tcpOptions
- hostAlias

Attribute name	Data type	Default value	Description
allowFromEndpointRef	List of references to top level httpEndpoint elements (comma-separated string).		Specify the identifier of one or more HTTP endpoints to restrict inbound traffic for this virtual host to the specified endpoints.
enabled	boolean	true	Enable this virtual host.
id	string		A unique configuration ID.

### allowFromEndpoint

Specify the identifier of one or more HTTP endpoints to restrict inbound traffic for this virtual host to the specified endpoints.

false

Attribute name	Data type	Default value	Description
accessLoggingRef	A reference to top level httpAccessLogging element (string).		HTTP access logging configuration for the endpoint.
enabled	boolean	true	Toggle the availability of an endpoint. When true, this endpoint will be activated by the dispatcher to handle HTTP requests.
host	string	localhost	IP address, domain name server (DNS) host name with domain name suffix, or just the DNS host name, used by a client to request a resource. Use '*' for all available network interfaces.

Attribute name	Data type	Default value	Description
httpOptionsRef	A reference to top level httpOptions element (string).	defaultHttpOptions	HTTP protocol options for the endpoint.
httpPort	int Minimum: -1 Maximum: 65535		The port used for client HTTP requests. Use -1 to disable this port.
httpsPort	int Minimum: -1 Maximum: 65535		The port used for client HTTP requests secured with SSL (https). Use -1 to disable this port.
id	string		A unique configuration ID.
onError	<ul style="list-style-type: none"> <li>• IGNORE</li> <li>• FAIL</li> <li>• WARN</li> </ul>	WARN	<p>Action to take after a failure to start an endpoint.</p> <p><b>IGNORE</b> Server will not issue any warning and error messages when it incurs a configuration error.</p> <p><b>FAIL</b> Server will issue a warning or error message on the first error occurrence and then stop the server.</p> <p><b>WARN</b> Server will issue warning and error messages when it incurs a configuration error.</p>
sslOptionsRef	A reference to top level sslOptions element (string).		SSL protocol options for the endpoint.
tcpOptionsRef	A reference to top level tcpOptions element (string).	defaultTCPOptions	TCP protocol options for the endpoint.

#### **allowFromEndpoint > accessLogging**

HTTP access logging configuration for the endpoint.

false

Attribute name	Data type	Default value	Description
enabled	boolean	true	Enable access logging.
filePath	Path to a file	\${server.output.dir}/logs/http_access.log	Directory path and name of the access log file. Standard variable substitutions, such as \${server.output.dir}, can be used when specifying the directory path.

Attribute name	Data type	Default value	Description
logFormat	string	%h %u %{t}W "%r" %s %b	Specifies the log format that is used when logging client access information.
maxFileSize	int Minimum: 0	20	Maximum size of a log file, in megabytes, before being rolled over; a value of 0 means no limit.
maxFiles	int Minimum: 0	2	Maximum number of log files that will be kept, before the oldest file is removed; a value of 0 means no limit.

**allowFromEndpoint > httpOptions**

HTTP protocol options for the endpoint.

false

Attribute name	Data type	Default value	Description
keepAliveEnabled	boolean	true	Enables persistent connections (HTTP keepalive). If true, connections are kept alive for reuse by multiple sequential requests and responses. If false, connections are closed after the response is sent.
maxKeepAliveRequests	int Minimum: -1	100	Maximum number of persistent requests that are allowed on a single HTTP connection if persistent connections are enabled. A value of -1 means unlimited.
persistTimeout	A period of time with second precision	30s	Amount of time that a socket will be allowed to remain idle between requests. This setting only applies if persistent connections are enabled. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
readTimeout	A period of time with second precision	60s	Amount of time to wait for a read request to complete on a socket after the first read occurs. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
removeServerHeader	boolean	false	Removes server implementation information from HTTP headers and also disables the default Liberty profile welcome page.
writeTimeout	A period of time with second precision	60s	Amount of time to wait on a socket for each portion of the response data to be transmitted. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

#### **allowFromEndpoint > sslOptions**

SSL protocol options for the endpoint.

false

Attribute name	Data type	Default value	Description
sessionTimeout	A period of time with second precision	1d	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

Attribute name	Data type	Default value	Description
sslRef	A reference to top level ssl element (string).		The default SSL configuration repertoire. The default value is defaultSSLSettings.
suppressHandshakeErrors	boolean	false	Disable logging of SSL handshake errors. SSL handshake errors can occur during normal operation, however these messages can be useful when SSL is behaving unexpectedly.

### allowFromEndpoint > tcpOptions

TCP protocol options for the endpoint.

false

Attribute name	Data type	Default value	Description
inactivityTimeout	A period of time with millisecond precision	60s	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
soReuseAddr	boolean	true	Enables immediate rebind to a port with no active listener.

### hostAlias

Associate a host and port with this virtual host, using the host:port syntax. The specified host can be an IP address, domain name server (DNS) hostname with a domain name suffix, the DNS hostname, or \* for a wildcard match on all hostnames. Note that IPv6 addresses must be enclosed in [].

false

string

## WAS JMS Endpoint (wasJmsEndpoint)

Configuration properties for WAS JMS incoming connection requests.

- sslOptions
- tcpOptions

Attribute name	Data type	Default value	Description
enabled	boolean	true	Toggle the availability of WAS JMS Endpoint.

Attribute name	Data type	Default value	Description
host	string	localhost	IP address, domain name server (DNS) host name with domain name suffix, or just the DNS host name, used by a client to request a resource. Use '*' for all available network interfaces.
sslOptionsRef	A reference to top level sslOptions element (string).		SSL protocol options for the WAS JMS endpoint.
tcpOptionsRef	A reference to top level tcpOptions element (string).	defaultTCPOptions	TCP protocol options for the WAS JMS endpoint.
wasJmsPort	int Minimum: -1 Maximum: 65535	7276	The port used for WAS JMS client messaging application connection requests. Use -1 to disable this port.
wasJmsSSLPort	int Minimum: -1 Maximum: 65535	7286	The port used for WAS JMS client messaging application connection requests secured with SSL. Use -1 to disable this port.

### sslOptions

SSL protocol options for the WAS JMS endpoint.

false

Attribute name	Data type	Default value	Description
sessionTimeout	A period of time with second precision	1d	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
sslRef	A reference to top level ssl element (string).		The default SSL configuration repertoire. The default value is defaultSSLSettings.
suppressHandshakeErrors	boolean	false	Disable logging of SSL handshake errors. SSL handshake errors can occur during normal operation, however these messages can be useful when SSL is behaving unexpectedly.

### tcpOptions

TCP protocol options for the WAS JMS endpoint.

false

Attribute name	Data type	Default value	Description
inactivityTimeout	A period of time with millisecond precision	60s	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
soReuseAddr	boolean	true	Enables immediate rebind to a port with no active listener.

### WAS JMS Outbound (wasJmsOutbound)

Configuration properties for WAS JMS outgoing connection requests.

- sslOptions
- tcpOptions

Attribute name	Data type	Default value	Description
id	string		The name of the WAS JMS outbound.
sslOptionsRef	A reference to top level sslOptions element (string).		SSL protocol options for WAS JMS outbound
tcpOptionsRef	A reference to top level tcpOptions element (string).	defaultTCPOptions	TCP protocol options for WAS JMS outbound
useSSL	boolean	false	Set the value to true to enable the secure communication channel

### sslOptions

SSL protocol options for WAS JMS outbound

false

Attribute name	Data type	Default value	Description
sessionTimeout	A period of time with second precision	1d	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
sslRef	A reference to top level ssl element (string).		The default SSL configuration repertoire. The default value is defaultSSLSettings.
suppressHandshakeErrors	boolean	false	Disable logging of SSL handshake errors. SSL handshake errors can occur during normal operation, however these messages can be useful when SSL is behaving unexpectedly.

### tcpOptions

TCP protocol options for WAS JMS outbound

false

Attribute name	Data type	Default value	Description
inactivityTimeout	A period of time with millisecond precision	60s	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
soReuseAddr	boolean	true	Enables immediate rebind to a port with no active listener.

## Web Container Application Security (webAppSecurity)

Configures web container application security.

Attribute name	Data type	Default value	Description
allowAuthenticationFailOverToAuthMethod	<ul style="list-style-type: none"> <li>• FORM</li> <li>• BASIC</li> </ul>		<p>Specifies the authentication fail over method that will be used when the certificate authentication fails. Valid values are BASIC and FORM.</p> <p><b>FORM</b> %allowAuthenticationFailOverToAuthMethod</p> <p><b>BASIC</b> %allowAuthenticationFailOverToAuthMethod</p>
allowFailOverToBasicAuth	boolean	false	<p>Specifies whether to fail over to basic authentication when certificate authentication fails. The equivalent custom property in the full application server profile is com.ibm.wsspi.security.web.failOverToBasicAuth</p>
allowLogoutPageRedirectToAnyHost	boolean	false	<p>Warning, security risk: Setting this property to true may open your systems to potential URL redirect attacks. If set to true, any host can be specified for the logout page redirect. If set to false, and the logout page points to a different host, or one not listed in the logout page redirect domain list, then a generic logout page is displayed. The equivalent custom property in the full application server profile is com.ibm.websphere.security.allowAnyLogoutE</p>

Attribute name	Data type	Default value	Description
displayAuthenticationRealm	boolean	false	Warning, security risk: if this property is set to true, and the user registry's realm name contains sensitive information, it is displayed to the user. For example, if an LDAP configuration is used, the LDAP server hostname and port are displayed. This configuration controls what the HTTP basic authentication login window displays when the realm name is not defined in the application web.xml. If the realm name is defined in the application web.xml file, this property is ignored. If set to true, the realm name displayed will be the user registry realm name for the LTPA authentication mechanism. If set to false, the realm name displayed will be "Default Realm". The equivalent custom property in the full application server profile is <code>com.ibm.websphere.security.displayRealm</code> .
httpOnlyCookies	boolean	true	Specifies whether the HTTP only (HttpOnly) cookies option is enabled.
includePathInWASReqURL	boolean	false	Setting the Path parameter can allow the client/browser to manage multiple WASReqURL cookies during multiple concurrent logins on the same user agent. The equivalent custom property in the full application server profile is <code>com.ibm.websphere.security.setContextRoot</code> .
loginFormURL	string		Specifies the global URL of a form login page including the root context. The form login page must be part of the WAR file. If a form login application does not specify the form login page in the web.xml file, it uses the global form login URL.

Attribute name	Data type	Default value	Description
logoutOnHttpSessionExpire	boolean	false	Specifies whether users will be logged out after the HTTP session timer expires. If set to false, the user credential will stay active until the Single Sign-On token timeout occurs. The equivalent custom property in the full application server profile is <code>com.ibm.ws.security.web.logoutOnHTTPSession</code>
logoutPageRedirectDomainNames	String		A pipe ( ) separated list of domain names that are allowed for the logout page redirect (localhost is implied). The equivalent custom property in the full application server profile is <code>com.ibm.websphere.security.logoutExitPageDomainNames</code>
postParamCookieSize	int	16384	Size of the POST parameter cookie. If the size of the cookie is larger than the browser limit, unexpected behavior may occur. The value of this property must be a positive integer and represents the maximum size of the cookie in bytes. The equivalent custom property in the full application server profile is <code>com.ibm.websphere.security.util.postParamMaxCookieSize</code>
postParamSaveMethod	<ul style="list-style-type: none"> <li>• Cookie</li> <li>• Session</li> <li>• None</li> </ul>	Cookie	<p>Specifies where POST parameters are stored upon redirect. Valid values are cookie (POST parameters are stored in a cookie), session (POST parameters are stored in the HTTP Session) and none (POST parameters are not preserved). The equivalent custom property in the full application server profile is <code>com.ibm.websphere.security.util.postParamSaveMethod</code></p> <p><b>Cookie</b>    Cookie</p> <p><b>Session</b>    Session</p> <p><b>None</b>    None</p>

Attribute name	Data type	Default value	Description
preserveFullyQualifiedReferrer	boolean	false	Warning, security risk: Setting this to true may open your systems to potential URL redirect attacks. This property specifies whether the fully qualified referrer URL for form login redirects is preserved. If false, the host for the referrer URL is removed and the redirect is to localhost. The equivalent custom property in the full application server profile is <code>com.ibm.websphere.security.util.fullyQualifiedReferrer</code> .
singleSignonEnabled	boolean	true	Specifies whether single sign-on is enabled.
ssoCookieName	string	LtpaToken2	Customizes the SSO cookie name. A custom cookie name allows you to logically separate authentication between SSO domains and to enable customized authentication to a particular environment. Before setting this value, consider that setting a custom cookie name can cause an authentication failure. For example, a connection to a server that has a custom cookie property set sends this custom cookie to the browser. A subsequent connection to a server that uses either the default cookie name or a different cookie name, is not able to authenticate the request via a validation of the in-bound cookie. The equivalent custom property in the full application server profile is <code>com.ibm.websphere.security.customSSOCookieName</code> .
ssoDomainNames	string		A pipe ( ) separated list of domain names that SSO Cookies should be presented. The equivalent custom property in the full application server profile is <code>com.ibm.ws.security.config.SingleSignonConfig</code> .

Attribute name	Data type	Default value	Description
ssoRequiresSSL	boolean	false	Specifies whether a SSO cookie is sent over SSL. The equivalent property in the full application server profile is requiresSSL.
ssoUseDomainFromURL	boolean	false	Specifies whether to use the domain name from the request URL for the cookie domain.
trackLoggedOutSSOCookies	boolean	false	Specifies whether to track LTPA single signon tokens that are logged out on a server so that it can not be reused on the same server.
useAuthenticationDataForUnprotectedResource	boolean	true	Specifies whether authentication data can be used when accessing an unprotected resource. The unprotected resource can access validated authenticated data that it previously could not access. This option enables the unprotected resource to call the getRemoteUser, isUserInRole, and getUserPrincipal methods to retrieve an authenticated identity. The equivalent custom property in the full application server profile is com.ibm.wsspi.security.webAuthReq=pers
useOnlyCustomCookieName	boolean	false	Specifies whether to use only the custom cookie name.
wasReqURLRedirectDomainNames	String		A pipe (!) separated list of domain names that are allowed for the WASReqURL page redirect. The hostname found on the form login request is implied.
webAlwaysLogin	boolean	false	Specifies whether the login() method will throw an exception when an identity has already been authenticated.

## Web Application (webApplication)

Defines the properties of a web application.

- application-bnd
  - security-role
  - group

- run-as
- special-subject
- user
- classloader
  - commonLibrary
    - file
    - fileset
    - folder
  - privateLibrary
    - file
    - fileset
    - folder

Attribute name	Data type	Default value	Description
autoStart	boolean	true	Indicates whether or not the server automatically starts the application.
contextRoot	string		Context root of an application.
id	string		A unique configuration ID.
location	A file, directory or url.		Location of an application expressed as an absolute path or a path relative to the server-level apps directory.
name	string		Name of an application.
suppressUncoveredHttpMethodWarning	boolean	false	Option to suppress uncovered HTTP method warning message during application deployment.

### application-bnd

Binds general deployment information included in the application to specific resources.

false

Attribute name	Data type	Default value	Description
version	string		Version of the application bindings specification.

### application-bnd > security-role

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	string		Name of a security role.

### application-bnd > security-role > group

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		Group access ID
id	string		A unique configuration ID.
name	string		Name of a group possessing a security role.

**application-bnd > security-role > run-as**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
password	Reversably encoded password (string)		Password of a user required to access a bean from another bean. The value can be stored in clear text or encoded form. To encode the password, use the securityUtility tool with the encode option.
userid	string		ID of a user required to access a bean from another bean.

**application-bnd > security-role > special-subject**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
type	<ul style="list-style-type: none"><li>• EVERYONE</li><li>• ALL_AUTHENTICATED_USERS</li></ul>		One of the following special subject types: ALL_AUTHENTICATED_USERS, EVERYONE.  <b>EVERYONE</b> Everyone  <b>ALL_AUTHENTICATED_USERS</b> All authenticated users

**application-bnd > security-role > user**

A unique configuration ID.

false

Attribute name	Data type	Default value	Description
access-id	string		A user access ID in the general form user:realmName/userUniqueId. A value will be generated if one is not specified.
id	string		A unique configuration ID.
name	string		Name of a user possessing a security role.

### classloader

Defines the settings for an application classloader.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
classProviderRef	List of references to top level resourceAdapter elements (comma-separated string).		List of class provider references. When searching for classes or resources, this class loader will delegate to the specified class providers after searching its own class path.
commonLibraryRef	List of references to top level library elements (comma-separated string).		List of library references. Library class instances are shared with other classloaders.
delegation	<ul style="list-style-type: none"> <li>parentFirst</li> <li>parentLast</li> </ul>	parentFirst	Controls whether parent classloader is used before or after this classloader. If parent first is selected then delegate to immediate parent before searching the classpath. If parent last is selected then search the classpath before delegating to the immediate parent.  <b>parentFirst</b> Parent first  <b>parentLast</b> Parent last
privateLibraryRef	List of references to top level library elements (comma-separated string).		List of library references. Library class instances are unique to this classloader, independent of class instances from other classloaders.

**classloader > commonLibrary**

List of library references. Library class instances are shared with other classloaders.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
id	string		A unique configuration ID.
name	string		Name of shared library for administrators

**classloader > commonLibrary > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**classloader > commonLibrary > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).

Attribute name	Data type	Default value	Description
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**classloader > commonLibrary > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

**classloader > privateLibrary**

List of library references. Library class instances are unique to this classloader, independent of class instances from other classloaders.

false

Attribute name	Data type	Default value	Description
apiTypeVisibility	string	spec,ibm-api,api	The types of API package this library's class loader will be able to see, as a comma-separated list of any combination of the following: spec, ibm-api, api, third-party.
description	string		Description of shared library for administrators
filesetRef	List of references to top level fileset elements (comma-separated string).		Id of referenced Fileset
id	string		A unique configuration ID.
name	string		Name of shared library for administrators

**classloader > privateLibrary > file**

Id of referenced File

false

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
name	Path to a file		Fully qualified filename

**classloader > privateLibrary > fileset**

Id of referenced Fileset

false

Attribute name	Data type	Default value	Description
caseSensitive	boolean	true	Boolean to indicate whether or not the search should be case sensitive (default: true).
dir	Path to a directory	\${server.config.dir}	The base directory to search for files.
excludes	string		The comma or space separated list of file name patterns to exclude from the search results, by default no files are excluded.
id	string		A unique configuration ID.
includes	string	*	The comma or space separated list of file name patterns to include in the search results (default: *).
scanInterval	A period of time with millisecond precision	0	Scanning interval to check the fileset for changes as a long with a time unit suffix h-hour, m-minute, s-second, ms-millisecond (e.g. 2ms or 5s). Disabled (scanInterval=0) by default. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

**classloader > privateLibrary > folder**

Id of referenced folder

false

Attribute name	Data type	Default value	Description
dir	Path to a directory		Directory or folder to be included in the library classpath for locating resource files
id	string		A unique configuration ID.

## Web Container (webContainer)

Configuration for the web container.

Attribute name	Data type	Default value	Description
allowExpressionFactoryPerApp	boolean	false	Toggle to load the ExpressionFactory that is set by the application. Enable this custom property if you are using a custom EL implementation (for example, JUEL) that needs to set its own ExpressionFactory.
allowIncludeSendError	boolean	false	Allow RequestDispatch to send errors on Include methods. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.allowincludesend
asyncMaxSizeTaskPool	int	5000	Maximum size of tasks in the Async task pool before automatically purging canceled tasks. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.asyncmaxsizetask
asyncPurgeInterval	int	30000	Time interval to wait between each required purge of the cancelled task pool. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.asyncpurgeinterval
asyncTimeoutDefault	int	30000	Async servlet timeout value used when a timeout value has not been explicitly specified. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.asynctimeoutdefa
asyncTimerThreads	int	2	Maximum number of threads to use for async servlet timeout processing. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.asynctimerthreads

Attribute name	Data type	Default value	Description
channelWriteType	string	async	When set to 'sync', responses will be written synchronously; otherwise, responses will be written asynchronously. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.channelwritetype.
copyAttributesKeySet	boolean	false	Web container will return an enumeration of a copy of the list of attributes to the servlet to avoid a concurrent access error by the servlet. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.copyattributeskeyset.
decodeUrlAsUtf8	boolean	true	Decode URLs using an encoding setting of UTF-8.
decodeUrlPlusSign	boolean	false	Decode the plus sign when it is part of the URL. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.decodeurlplussign.
defaultHeadRequestBehavior	boolean	false	Restore the behavior where the HEAD request is not subject to the security constraint defined for the GET method. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.DefaultHeadRequestBehavior.
defaultTraceRequestBehavior	boolean	false	Restore HTTP TRACE processing. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.DefaultTraceRequestBehavior.
deferServletLoad	boolean	true	Defer servlet loading and initialization until the first request.
deferServletRequestListenerDestroyOnError	boolean	false	Toggle if you want to defer ServletRequestListener destroy when there is an error serving the request. The default value is false. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.deferServletRequestListenerDestroyOnError.
directoryBrowsingEnabled	boolean	false	Enable directory browsing of an application.

Attribute name	Data type	Default value	Description
disableXPoweredBy	boolean	false	Disable setting the X-Powered-By header. The equivalent custom property in the full application server profile is <code>com.ibm.ws.webcontainer.disablexpoweredby</code>
disallowAllFileServing	boolean	false	Disables all file serving by applications. The equivalent custom property in the full application server profile is <code>com.ibm.ws.webcontainer.disallowAllFileServing</code>
disallowServeServletsByClassName	boolean	true	Disallows the use of <code>serveServletsByClassNameEnabled</code> on the application server level. The equivalent custom property in the full application server profile is <code>com.ibm.ws.webcontainer.disallowserveservletsbyclassname</code>
dispatcherRethrowsError	boolean	true	Web container will re-throw errors allowing interested resources to process them. The equivalent custom property in the full application server profile is <code>com.ibm.ws.webcontainer.dispatcherRethrowsError</code>
doNotServeByClassName	string		A semi-colon delimited list of classes to be completely disallowed from being served by classname. The equivalent custom property in the full application server profile is <code>com.ibm.ws.webcontainer.donotservebyclassname</code>
emptyServletMappings	boolean	false	Toggle if you want to return an empty collection, instead of null, when no servlet mappings are added. The default value is false. The equivalent custom property in the full application server profile is <code>com.ibm.ws.webcontainer.emptyServletMappings</code>
enableDefaultIsELIgnoredInTags	boolean	false	Always evaluate whether to ignore EL expressions in tag files. If parent JSP files have different <code>isELIgnored</code> settings, the setting will be re-evaluated in the tag file. The equivalent custom property in the full application server profile is <code>com.ibm.ws.jsp.enabledefaultisignoredintags</code>

Attribute name	Data type	Default value	Description
enableErrorExceptionTypeFirst	boolean	false	Web container is updated to search and use the exception-type before the error-code. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.enableErrorExceptionTypeFirst
enableJspMappingOverride	boolean	false	Allow the JSP mapping to be overridden so that the application can serve the JSP contents itself. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.enablejspmappingoverride
enableMultiReadOfPostData	boolean	false	Retain post data for multiple read accesses. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.enablemultireadofpostdata
exposeWebInfOnDispatch	boolean	false	If true, a servlet can access files in the WEB-INF directory. If false (default), a servlet cannot access files the WEB-INF directory.
fileServingEnabled	boolean	true	Enable file serving if this setting was not explicitly specified for the application.
fileWrapperEvents	boolean	false	Web container will generate SMF and PMI data when serving the static files. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.fileWrapperEvents
httpsIndicatorHeader	string		For SSL offloading, set to the name of the HTTP header variable inserted by the SSL accelerator/proxy/load balancer.
ignoreSemiColonOnRedirectToWelcomePage	boolean	false	Toggle to ignore the trailing semi-colon when redirecting to the welcome page. The default value is false. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.ignoreSemiColonOnRedirectToWelcomePage

Attribute name	Data type	Default value	Description
ignoreSessiononStaticFileRequests	boolean	false	Improves performance by preventing the web container from accessing a session for static file requests involving filters. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.IgnoreSessiononStaticFileRequests
invokeFilterInitAtStartup	boolean	true	Web container will call the filter's init() method at application startup. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.invokeFilterInitAtStartup
listeners	string		A comma separated list of listener classes.
logServletContainerInitializationClassLoadingErrors	boolean	false	Log servlet container class loading errors as warnings rather than logging them only when debug is enabled. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.logServletContainerInitializationClassLoadingErrors
metaInfResourcesCacheSize	int	20	Initial size (number of entries) of the meta-inf resource cache. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.metaInfResourcesCacheSize
parseUtf8PostData	boolean	false	Web container will detect non URL encoded UTF-8 post data and include it in the parameter values. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.parseUtf8PostData
serveServletsByClassnameEnabled	boolean	false	Enable servlets to be accessed in a web application using a class name if not explicitly specified.
setContentLengthOnClose	boolean	true	Toggle to set content length when an application explicitly closes the response. The default value is true; however, set this value to false if an application response contains double-byte characters.

Attribute name	Data type	Default value	Description
skipMetaInfResourcesProcessing	boolean	false	Do not search the meta-inf directory for application resources. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.skipmetainfresources.
suppressHtmlRecursiveErrors	boolean	false	Suppresses the exception information from appearing in the HTML output when there is a recursive error that cannot be handled by an application's configured error page. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.suppressHtmlRecursiveErrors.
symbolicLinksCacheSize	int	1000	Initial size of the symbolic link cache. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.SymbolicLinksCacheSize.
tolerateSymbolicLinks	boolean	false	Enables the web container to support the use of symbolic links. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.TolerateSymbolicLinks.
useSemiColonAsDelimiterInURI	boolean	false	Toggle to use the semi-colon as a delimiter in the request URI. The default value is false. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.useSemiColonAsDelimiterInURI.
xPoweredBy	string		Alternative string for the X-Powered-By header setting. The equivalent custom property in the full application server profile is com.ibm.ws.webcontainer.xpoweredby. There is no default value for this property. If the property is not set, the value of the X-Powered-By header is set to Servlet/<servlet spec version>, as defined by the Servlet specification.

## WLM Classification (wlmClassification)

Contains, as child elements, the classification rules WLM will use when classifying requests.

- httpClassification

Attribute name	Data type	Default value	Description
classificationName	string	null	Optional classification name
id	string		A unique configuration ID.

### httpClassification

An element representing a rule used by WLM for classifying incoming HTTP requests.

false

Attribute name	Data type	Default value	Description
host	string	*	Defines which host to map the transaction class to
method	string	*	Defines the HTTP method to map to
port	string	*	Defines which port to map the transaction class to
resource	string	*	Defines the URI to use when mapping transaction class
transactionClass	string		Defines the priority

## WebSphere MQ Messaging (wmqJmsClient)

WebSphere MQ messaging

Attribute name	Data type	Default value	Description
connectionConcurrency	int Minimum: 0	1	The maximum number of MDBs that can be supplied by each connection
id	string		A unique configuration ID.
logWriterEnabled	boolean	true	A flag to enable or disable the sending of a diagnostic trace to a LogWriter object provided by the application server
maxConnections	int Minimum: 0	50	The maximum number of connections to a WebSphere MQ queue manager
nativeLibraryPath	string		Absolute path to the location of the WebSphere MQ Java JNI library (mqjbnd.dll or equivalent)
reconnectionRetryCount	int Minimum: 0	5	The maximum number of attempts made to reconnect to a WebSphere MQ queue manager if a connection fails

Attribute name	Data type	Default value	Description
reconnectionRetryInterval	A period of time with millisecond precision	5m	The time, in milliseconds, that the WebSphere MQ feature waits before making another attempt to reconnect to a WebSphere MQ queue manager. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
startupRetryCount	int Minimum: 0	0	Number of times to retry creating a connection on startup
startupRetryInterval	A period of time with millisecond precision	30s	The time to wait, in milliseconds, between each retry attempt when connecting on startup. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.

## WS-AtomicTransaction (wsAtomicTransaction)

Configuration properties for the Web Services Atomic Transaction feature.

Attribute name	Data type	Default value	Description
clientAuth	boolean	false	Specifies whether additional client authentication is enabled for the WS-AtomicTransaction protocol when SSL is enabled.
externalURLPrefix	string		Optionally specifies the host and port address of a proxy server used to route the WS-AtomicTransaction protocol.

Attribute name	Data type	Default value	Description
sslEnabled	boolean	false	When set to true, WS-AtomicTransaction internal event messages sent between the WS-AT coordinator and participant are encrypted using SSL.
sslRef	A reference to top level ssl element (string).	defaultSSLConfig	Specifies the SSL configuration to be used for the WS-AtomicTransaction protocol when SSL is enabled.

## WS-Security Client (wsSecurityClient)

Web Services Security default configuration for client.

- encryptionProperties
- signatureProperties

Attribute name	Data type	Default value	Description
ws-security.callback-handler	string		Password callback handler implementation class.
ws-security.encryption.username	string		Alias used for accessing encryption keystore.
ws-security.password	Reversably encoded password (string)		User password information needed to create Username Token.
ws-security.signature.username	string		Alias used for accessing signature keystore.
ws-security.username	string		User information to create Username Token.

### encryptionProperties

Required encryption configuration.

false

Attribute name	Data type	Default value	Description
org.apache.ws.security.crypto.provider	string		The provider used to load certificates. Defaults to keystore provider.
org.apache.ws.security.crypto.file	string		The location of the keystore
org.apache.ws.security.crypto.keystore.alias	string		The default keystore alias to use, if none is specified.
org.apache.ws.security.crypto.keystore.password	Reversably encoded password (string)		Password to access keystore file.
org.apache.ws.security.crypto.keystore.private.password	Reversably encoded password (string)		The default password used to load the private key.
org.apache.ws.security.crypto.keystore.provider	string		The provider used to load keystores. Defaults to installed provider.
org.apache.ws.security.crypto.keystore.type	string		JKS, JCEKS or PKCS11

Attribute name	Data type	Default value	Description
org.apache.ws.security.crypto	string.truststore.file		The location of the truststore
org.apache.ws.security.crypto	ReversibleTrustStore password (string)		The truststore password.
org.apache.ws.security.crypto	string.truststore.type		The truststore type.
org.apache.ws.security.crypto	string.x509crl.file		The location of an (X509) CRL file to use.
org.apache.ws.security.crypto	string.provider	org.apache.ws.security.components.crypto.provider	Provides the URL to create Crypto instances. Defaults to "org.apache.ws.security.components.crypto.Mer...

### signatureProperties

Required signature configuration.

false

Attribute name	Data type	Default value	Description
org.apache.ws.security.crypto	string.cert.provider		The provider used to load certificates. Defaults to keystore provider.
org.apache.ws.security.crypto	string.file		The location of the keystore
org.apache.ws.security.crypto	string.keystore.alias		The default keystore alias to use, if none is specified.
org.apache.ws.security.crypto	ReversibleTrustStore password (string)		Password to access keystore file.
org.apache.ws.security.crypto	ReversibleTrustStore private password (string)		The default password used to load the private key.
org.apache.ws.security.crypto	string.keystore.provider		The provider used to load keystores. Defaults to installed provider.
org.apache.ws.security.crypto	string.keystore.type		JKS, JCEKS or PKCS11
org.apache.ws.security.crypto	string.truststore.file		The location of the truststore
org.apache.ws.security.crypto	ReversibleTrustStore password (string)		The truststore password.
org.apache.ws.security.crypto	string.truststore.type		The truststore type.
org.apache.ws.security.crypto	string.x509crl.file		The location of an (X509) CRL file to use.
org.apache.ws.security.crypto	string.provider	org.apache.ws.security.components.crypto.provider	Provides the URL to create Crypto instances. Defaults to "org.apache.ws.security.components.crypto.Mer...

## WS-Security Provider (wsSecurityProvider)

Web Services Security default configuration for provider.

- callerToken
- encryptionProperties
- samlToken

- audienceRestrictions
- signatureProperties

Attribute name	Data type	Default value	Description
ws-security.callback-handler	string		Password callback handler implementation class.
ws-security.enable.nonce.cache	boolean	true	Whether to cache UsernameToken nonces.
ws-security.encryption.username	string		Alias used for accessing encryption keystore.
ws-security.signature.username	string		Alias used for accessing signature keystore.
ws-security.username	string		User information to create Username Token.

### callerToken

Caller token.

false

Attribute name	Data type	Default value	Description
allowCustomCacheKey	boolean	true	Allow the generation of a custom cache key to access the authentication cache and get the subject.
groupIdIdentifier	string		Specifies a SAML attribute that is used as the name of the group that the authenticated principal is a member of. There is no default value.
includeTokenInSubject	boolean	true	Specifies whether to include a SAML assertion in the subject.
mapToUserRegistry	<ul style="list-style-type: none"> <li>• User</li> <li>• No</li> <li>• Group</li> </ul>	No	<p>Specifies how to map an identity to a registry user. The options are No, User, and Group. The default is No, and the user registry is not used to create the user subject.</p> <p><b>User</b> Map a SAML identity to a user defined in the registry</p> <p><b>No</b> Do not map a SAML identity to a user or group in the registry</p> <p><b>Group</b> Map a SAML identity to a group defined in the user registry</p>

Attribute name	Data type	Default value	Description
name	string		Specify token name. The options are Usenamtoken, X509token, Samltoken.
realmIdentifier	string		Specifies a SAML attribute that is used as the realm name. The default is issuer.
realmName	string		Specifies a realm name when mapToUserRegistry is set to No or Group.
userIdentifier	string		Specifies a SAML attribute that is used as the user principal name in the subject. The default is NameID assertion.
userUniqueIdentifier	string		Specifies a SAML attribute that is used as the unique user name as it applies to the WSCredential in the subject. The default is the same as the userIdentifier attribute value.

### encryptionProperties

Required encryption configuration.

false

Attribute name	Data type	Default value	Description
org.apache.ws.security.crypto.provider	string.cert.provider		The provider used to load certificates. Defaults to keystore provider.
org.apache.ws.security.crypto.keystore.file	string.file		The location of the keystore
org.apache.ws.security.crypto.keystore.alias	string.keystore.alias		The default keystore alias to use, if none is specified.
org.apache.ws.security.crypto.keystore.password	Reversible keystore password (string)		Password to access keystore file.
org.apache.ws.security.crypto.keystore.private.password	Reversible keystore private password (string)		The default password used to load the private key.
org.apache.ws.security.crypto.keystore.provider	string.keystore.provider		The provider used to load keystores. Defaults to installed provider.
org.apache.ws.security.crypto.keystore.type	string.keystore.type		JKS, JCEKS or PKCS11
org.apache.ws.security.crypto.truststore.file	string.truststore.file		The location of the truststore
org.apache.ws.security.crypto.truststore.password	Reversible truststore password (string)		The truststore password.
org.apache.ws.security.crypto.truststore.type	string.truststore.type		The truststore type.
org.apache.ws.security.crypto.x509crl.file	string.x509crl.file		The location of an (X509) CRL file to use.

Attribute name	Data type	Default value	Description
org.apache.ws.security.crypto.provider	string	org.apache.ws.security.components.crypto.provider	Specifies the name of the Crypto instances. Defaults to "org.apache.ws.security.components.crypto.M...

### samlToken

Specifies the properties that are used to evaluate the trustworthiness and validity of a SAML Assertion.

false

Attribute name	Data type	Default value	Description
clockSkew	A period of time with millisecond precision	5m	This is used to specify the allowed clock skew in minutes when validating the SAML token. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
requiredSubjectConfirmationMethod	bearer	bearer	Specify whether the Subject Confirmation Method is required in the SAML Assertion. Default is true. <b>bearer</b> bearer
timeToLive	A period of time with millisecond precision	30m	Specify the default life time of a SAML Assertion in the case it does not define the NoOnOrAfter condition. Default is 30 minutes. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
wantAssertionsSigned	boolean	true	Indicates a requirement for the <saml:Assertion> elements received by this service provider to be signed.

### samlToken > audienceRestrictions

Specify the allowed audiences of the SAML Assertion. Default is all audiences allowed.

false

string

### signatureProperties

Required signature configuration.

false

Attribute name	Data type	Default value	Description
org.apache.ws.security.crypto.provider	string.cert.provider		The provider used to load certificates. Defaults to keystore provider.
org.apache.ws.security.crypto.keystore.file	string.file		The location of the keystore
org.apache.ws.security.crypto.keystore.alias	string.keystore.alias		The default keystore alias to use, if none is specified.
org.apache.ws.security.crypto.keystore.password	string.keystore.password (string)		Password to access keystore file.
org.apache.ws.security.crypto.keystore.private.password	string.keystore.private.password (string)		The default password used to load the private key.
org.apache.ws.security.crypto.keystore.provider	string.keystore.provider		The provider used to load keystores. Defaults to installed provider.
org.apache.ws.security.crypto.keystore.type	string.keystore.type		JKS, JCEKS or PKCS11
org.apache.ws.security.crypto.truststore.file	string.truststore.file		The location of the truststore
org.apache.ws.security.crypto.truststore.password	string.truststore.password (string)		The truststore password.
org.apache.ws.security.crypto.truststore.type	string.truststore.type		The truststore type.
org.apache.ws.security.crypto.x509crl.file	string.x509crl.file		The location of an (X509) CRL file to use.
org.apache.ws.security.crypto.provider	string	org.apache.ws.security.components.crypto.provider	Provides the provider to use to create Crypto instances. Defaults to "org.apache.ws.security.components.crypto.Mer...

## WAS WebSocket Outbound (wsocOutbound)

Configuration properties for WAS WebSocket outgoing connection requests.

- httpOptions
- sslOptions
- tcpOptions

Attribute name	Data type	Default value	Description
httpOptionsRef	A reference to top level httpOptions element (string).	defaultHttpOptions	HTTP protocol options for WAS WebSocket outbound
sslOptionsRef	A reference to top level sslOptions element (string).		SSL protocol options for WAS WebSocket outbound
tcpOptionsRef	A reference to top level tcpOptions element (string).	defaultTCPOptions	TCP protocol options for WAS WebSocket outbound

## httpOptions

HTTP protocol options for WAS WebSocket outbound

false

Attribute name	Data type	Default value	Description
keepAliveEnabled	boolean	true	Enables persistent connections (HTTP keepalive). If true, connections are kept alive for reuse by multiple sequential requests and responses. If false, connections are closed after the response is sent.
maxKeepAliveRequests	int Minimum: -1	100	Maximum number of persistent requests that are allowed on a single HTTP connection if persistent connections are enabled. A value of -1 means unlimited.
persistTimeout	A period of time with second precision	30s	Amount of time that a socket will be allowed to remain idle between requests. This setting only applies if persistent connections are enabled. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
readTimeout	A period of time with second precision	60s	Amount of time to wait for a read request to complete on a socket after the first read occurs. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
removeServerHeader	boolean	false	Removes server implementation information from HTTP headers and also disables the default Liberty profile welcome page.

Attribute name	Data type	Default value	Description
writeTimeout	A period of time with second precision	60s	Amount of time to wait on a socket for each portion of the response data to be transmitted. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.

### sslOptions

SSL protocol options for WAS WebSocket outbound

false

Attribute name	Data type	Default value	Description
sessionTimeout	A period of time with second precision	1d	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). For example, specify 30 seconds as 30s. You can include multiple values in a single entry. For example, 1m30s is equivalent to 90 seconds.
sslRef	A reference to top level ssl element (string).		The default SSL configuration repertoire. The default value is defaultSSLSettings.
suppressHandshakeErrors	boolean	false	Disable logging of SSL handshake errors. SSL handshake errors can occur during normal operation, however these messages can be useful when SSL is behaving unexpectedly.

### tcpOptions

TCP protocol options for WAS WebSocket outbound

false

Attribute name	Data type	Default value	Description
inactivityTimeout	A period of time with millisecond precision	60s	Amount of time to wait for a read or write request to complete on a socket. This value is overridden by protocol-specific timeouts. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
soReuseAddr	boolean	true	Enables immediate rebind to a port with no active listener.

## z/OS Connect Data Transformer (zosConnectDataXform)

Defines a z/OS Connect data transformer.

Attribute name	Data type	Default value	Description
bindFileLoc	string		File system path where the bind files are located.
bindFileSuffix	string		Suffix name that is associated with the bind files.
id	string		A unique configuration ID.
pollingRate	A period of time with millisecond precision	2s	Rate at which the server checks for updates to data transformation related files such as bind or schema files. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
requestSchemaLoc	string		File system path where the request schema files are located.
requestSchemaSuffix	string		Suffix name that is associated with the request schema files.

Attribute name	Data type	Default value	Description
responseSchemaLoc	string		File system path where the response schema files are located.
responseSchemaSuffix	string		Suffix name that is associated with the response schema files.
updateTrigger	<ul style="list-style-type: none"> <li>• mbean</li> <li>• polled</li> <li>• disabled</li> </ul>	polled	<p>Update trigger for data transformation files such as bind and schema files.</p> <p><b>mbean</b> Server reloads data transformation files when prompted by an MBean called by an external program such as an integrated development environment or a management application.</p> <p><b>polled</b> Server scans for changes at the polling interval and reload any files that have detectable changes.</p> <p><b>disabled</b> Disables all update monitoring. Data transformation file changes will not be applied while the server is running.</p>

## z/OS Connect Interceptors (zosConnectInterceptors)

Bundles 1 to N interceptors.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
interceptorRef	List of references to top level auditInterceptor elements (comma-separated string).		The identifier of one or more interceptors.

## z/OS Connect Manager (zosConnectManager)

Defines global configuration settings for z/OS Connect.

- globalInterceptorsRef

Attribute name	Data type	Default value	Description
asyncRequestTimeout	A period of time with millisecond precision		<p>Timeout value that is associated with all service endpoints when processing asynchronous work. It specifies the time in milliseconds in which requests have to complete. This timeout value overrides the web container's <code>asyncTimeoutDefault</code> attribute value. If neither <code>asyncRequestTimeout</code> nor <code>asyncTimeoutDefault</code> are configured, the timeout used is the <code>asyncTimeoutDefault</code> attribute default value (i.e. 30 seconds). If <code>asyncRequestTimeout</code> is not configured, but the <code>asyncTimeoutDefault</code> attribute is, the <code>asyncTimeoutDefault</code>'s configured value is used. A timeout may occur at any time during z/OS Connect's processing of the request. The request might still be active after the timeout is detected and a response is sent to the client. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.</p>
globalAdminGroup	string		Administrative group name that is associated with all service endpoints. It is the name of the security group that the user needs to be in before administrative functions are permitted.
globalDataXformRef	A reference to top level <code>zosConnectDataXform</code> element (string).		Reference name that identifies the data transformation handler that is associated with all service endpoints.

Attribute name	Data type	Default value	Description
globalInvokeGroup	string		Invoke group name that is associated with all service endpoints. It contains the name of the security group that the user needs to be in before invoke calls are permitted.
globalOperationsGroup	string		Operations group name that is associated with all service endpoints. It is the name of the security group that the user needs to be in before operations such as start, stop, or status is permitted.
operationMode	<ul style="list-style-type: none"> <li>• SYNC</li> <li>• ASYNC</li> </ul>	ASYNC	<p>Specifies the mode in which all z/OS Connect requests are processed.</p> <p><b>SYNC</b> Synchronous mode of operation</p> <p><b>ASYNC</b> Asynchronous mode of operation</p>
preserveJsonObjectPayloadOrder	boolean	false	Indicates if the order of entries in a JSON object payload should be preserved. This setting applies to requests associated with all service endpoints.
preserveJsonPayloadCharForm	boolean	false	Indicates if the JSON payload's characters should flow unchanged through z/OS Connect during a service invocation and schema retrievals when using z/OS Connect's data transformer. When it is set to false, UTF-8 encoded characters might be converted to its respective escaped unicode representation. For this attribute to take effect, the attribute definition <code>preserveJsonObjectPayloadOrder</code> must be configured and set to true.
requireAuth	boolean	true	Indicates if users must provide security credentials in order for z/OS Connect to process requests. This setting applies to requests associated with all service endpoints.

Attribute name	Data type	Default value	Description
requireSecure	boolean	true	Indicates if requests must be made by using the secure HTTPS channel. This setting applies to requests associated with all service endpoints.
setUTF8ResponseEncoding	boolean	false	Indicates if the character encoding in the HTTP response should be set to UTF-8.

### globalInterceptorsRef

Reference name that identifies the set of configured interceptors that is associated with all service endpoints. If service endpoints do not require global interceptors association, the runGlobalInterceptors attribute under the zosConnectService element can be set to false.

false

tokenType

## z/OS Connect Endpoint (zosConnectService)

Defines the configuration settings for a service endpoint.

- interceptorsRef

Attribute name	Data type	Default value	Description
adminGroup	string		Administrative group name that is associated with a service endpoint. It is the name of the security group that the user needs to be in before administrative functions are permitted. If it is configured along with its global counterpart globalAdminGroup that is defined under element zosConnectManager, the value defined under adminGroup is used.
dataXformRef	A reference to top level zosConnectDataXform element (string).		Reference name that identifies the data transformation handler that is associated with a service endpoint. If configured along with its global data transformation handler counterpart globalDataXformRef that is defined under element zosConnectManager, the data transformer defined for the service endpoint is used.
id	string		A unique configuration ID.

Attribute name	Data type	Default value	Description
invokeGroup	string		Invoke group name that is associated with a service endpoint. It contains the name of the security group that the user needs to be in before invoke calls are permitted. If it is configured along with its global counterpart globalInvokeGroup that is defined under element zosConnectManager, the value defined under invokeGroup is used.
invokeURI	string		<p>URI or list of comma-separated URIs to associate with a service endpoint. InvokeURIs can end with a wildcard character in the form /a/b/* or x/y* to generically match a service endpoint invocation. Specifying multiple wildcard characters (i.e. /a/b/**) or wildcard characters in the middle of the requestURI (i.e. /a/*/c) is not supported. If service endpoints with configured invokeURIs using the wildcard character are associated with overlapping invokeURIs, the service endpoint associated with the most specific invokeURI is matched. For instance, if a service endpoint request is issued with the following:  https://host:port/a/b/c  going to a server with the following configuration:  service1 -&gt;  invokeURI="/a/b/c/*" and  service2 -&gt;  invokeURI="/a/b/*", z/OS Connect will match the request to service1. Configured invokeURI entries must start with the / character. The use of an invokeURI is equivalent to a service request where the action=invoke query parameter is specified.</p>

Attribute name	Data type	Default value	Description
operationsGroup	string		Operations group name that is associated with a service endpoint. It is the name of the security group that the user needs to be in before operations such as start, stop, or status is permitted. If it is configured along with its global counterpart, globalOperationsGroupdefined under element zosConnectManager, the value defined under operationsGroup is used.
requireAuth	boolean		Indicates if users must provide security credentials in order for z/OS Connect to process requests associated with a service endpoint. If it is configured along with its global counterpart requireAuth that is defined under the zosConnectManager element, the value defined for the service endpoint is used.
requireSecure	boolean		Indicates if requests associated with a service endpoint must be made by using the secure HTTPS channel. If it is configured along with its global counterpart requireSecure that is defined under the zosConnectManager element, the value defined for the service endpoint is used.
runGlobalInterceptors	boolean	true	Indicates whether global interceptors should run for requests associated with a service endpoint. By default z/OS Connect processes all global and service endpoint specific interceptors .

Attribute name	Data type	Default value	Description
serviceAsyncRequestTimeout	A period of time with millisecond precision		Timeout value that is associated with a service endpoint when processing asynchronous work. It specifies the time in milliseconds in which requests have to complete. This timeout value overrides the web container's <code>asyncTimeoutDefault</code> attribute value. If neither <code>asyncRequestTimeout</code> nor <code>asyncTimeoutDefault</code> are configured, the timeout used is the <code>asyncTimeoutDefault</code> attribute default value (i.e. 30 seconds). If <code>asyncRequestTimeout</code> is not configured, but the <code>asyncTimeoutDefault</code> attribute is, the <code>asyncTimeoutDefault</code> 's configured value is used. If configured along with its global counterpart: <code>asyncRequestTimeout</code> defined under element <code>zosConnectManager</code> , the value defined under <code>serviceAsyncRequestTimeout</code> is used. A timeout may occur at any time during z/OS Connect's processing of the request. The request may still be active after the timeout is detected and a response is sent to the client. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
serviceDescription	string		Description that is associated with a service endpoint.
serviceGroupingName	string		Name that can be used to group or associate a set of service endpoints together.

Attribute name	Data type	Default value	Description
serviceName	string		Name that is associated with a service endpoint. This name identifies a service endpoint to a client.
serviceRef	A reference to top level localAdaptersConnectService element (string).		Reference name that identifies the service endpoint that is registered with z/OS Connect.

### interceptorsRef

Reference name that identifies the set of configured interceptors that is associated with a service endpoint. If it is configured along with its global interceptors counterpart globalInterceptorsRef that is defined under the zosConnectManager element, z/OS Connect processes both sets of interceptors. If the runGlobalInterceptors attribute for the service endpoint is set to false, z/OS connect will only process the set of interceptors configured for the service endpoint.

false

tokenType

## z/OS Connect REST Client (zosConnectServiceRestClient)

Allows requests to be routed from z/OS Connect to a remote REST endpoint.

- basicAuth

Attribute name	Data type	Default value	Description
basicAuthRef	A reference to top level zosConnectServiceRestClientBasicAuth element (string).	BasicAuth	Reference name that identifies the basic authentication data to be used for connecting to a remote REST endpoint.
connectionTimeout	A period of time with millisecond precision	30s	The connection timeout specifies the amount of time that the client will attempt to establish a connection to the remote endpoint before it times out. If the timeout value is set to 0, the client will attempt to open a connection indefinitely. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
host	string		IP address, domain name server (DNS) host name with domain name suffix, or just the DNS host name, used to route the request.

Attribute name	Data type	Default value	Description
httpMethod	string		Name of the HTTP method to be used when routing HTTP requests. If no method is specified, the method used is the one in the original request.
id	string		A unique configuration ID.
port	string		Port used for routing HTTP or HTTPS requests.
receiveTimeout	A period of time with millisecond precision	60s	The receive timeout specifies the amount of time that the client will wait for a response from the remote endpoint before it times out. If the timeout value is set to 0, the client will wait for a response indefinitely. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), seconds (s), or milliseconds (ms). For example, specify 500 milliseconds as 500ms. You can include multiple values in a single entry. For example, 1s500ms is equivalent to 1.5 seconds.
sslCertsRef	A reference to top level keyStore element (string).		An SSL repertoire with an ID, a defined keystore, and truststore.
uri	string		URI that identifies the resource to contact when routing HTTP requests. If no URI is specified everything after the port number from the original request is used.

### basicAuth

Reference name that identifies the basic authentication data to be used for connecting to a remote REST endpoint.

false

Attribute name	Data type	Default value	Description
password	Reversably encoded password (string)		Password of the user under which the request will be routed. The value can be stored in clear text or encoded. It is recommended that the password be encoded. To do so, use the securityUtility shipped with WebSphere Liberty profile.

Attribute name	Data type	Default value	Description
userName	string		Name of the user under which the request will be routed.

## z/OS Connect Rest Client Basic Authentication (zosConnectServiceRestClientBasicAuth)

Basic authentication data for connecting to a remote REST endpoint.

Attribute name	Data type	Default value	Description
id	string		A unique configuration ID.
password	Reversably encoded password (string)		Password of the user under which the request will be routed. The value can be stored in clear text or encoded. It is recommended that the password be encoded. To do so, use the securityUtility shipped with WebSphere Liberty profile.
userName	string		Name of the user under which the request will be routed.

## WOLA (zosLocalAdapters)

WebSphere Optimized Local Adapters.

Attribute name	Data type	Default value	Description
useCicsTaskUserId	boolean	false	If security is enabled in the WOLA client, this setting controls which user ID is propagated to this Liberty profile server when a WOLA request is sent from the client to the server. If you enable this setting, the user ID of the task that makes the request is propagated. If you do not enable this setting, the user ID of the client address space is propagated. This setting is applicable only to CICS clients.
wolaGroup	string		The WOLA group name is the first part of the 3-part WOLA name. The name cannot contain lowercase letters.

Attribute name	Data type	Default value	Description
wolaName2	string		The 2nd part of the 3-part WOLA name. The name cannot contain lowercase letters.
wolaName3	string		The 3rd part of the 3-part WOLA name. The name cannot contain lowercase letters.

## z/OS Logging (zosLogging)

Configuration properties for logging on z/OS.

Attribute name	Data type	Default value	Description
enableLogToMVS	boolean	false	Enable routing of USS-started server messages to the MVS console.
hardCopyMessage	string		A comma-separated list of message IDs to be written to the hardcopy log.
wtoMessage	string		A comma-separated list of message IDs to be written to operator.

## WLM Native Enclave Manager (zosWorkloadManager)

WLM Native Enclave Manager Configuration.

Attribute name	Data type	Default value	Description
collectionName	string	\${wlp.server.name}	A collection name to be used for classifying work requests. The name is supplied to native services IWMCLSFY or __server_classify. Only the first 18 characters will be used.

---

## Liberty: Feature management

Features are the units of functionality by which you control the pieces of the runtime environment that are loaded into a particular server.

Use the configuration file `server.xml` to declare which features you want to load. The set of features is enclosed within the `<featureManager>` element, and each feature within the `<feature>` subelement. For example:

```
<server>
  <featureManager>
    <feature>servlet-3.0</feature>
    <feature>localConnector-1.0</feature>
  </featureManager>
</server>
```

You can specify any feature in the server configuration file. Some features include other features within them. The same feature can be included in one or more other features. At run time, the feature manager computes the combined list of content that is required to support the requested set of features.

For information about the main available features, see “Liberty features” on page 826. For information about the restrictions that apply to each feature, see “Liberty:Runtime environment known issues and restrictions” on page 2333.

## Dynamic changes to feature configuration

When you change the feature configuration, the feature manager recalculates the list of required bundles, stops and uninstalls those bundles that are no longer required, and installs and starts any additions. Therefore, all features are designed to cope with other features that are being dynamically added or removed.

8.5.5.4

### Singleton Features

With the delivery of the first set of features for Java EE 7, there are now two versions of the same feature:

- `servlet-3.0`
- `servlet-3.1`

Unlike other application servers, you can choose which version of this feature to use in a server configuration. `servlet-3.0` preserves behavior for existing applications, while `servlet-3.1` provides new capabilities for new or modified applications. Although there is a choice of specification versions, no additional configuration properties are required, or provided, to control individual differences between the two versions.

The servlet feature is a singleton feature, which means that you can configure only one version for use in a server: either `servlet-3.0` or `servlet-3.1`. If you have applications that need different versions of the servlet feature, you must deploy them in different servers. Many other features include the servlet feature as a dependency. In the WebSphere Liberty product, these features have been updated to work with either version. This ensures that you can configure a complete “stack” of features when you use `servlet-3.1`, but features from other sources might not have been updated to “tolerate” `servlet-3.1`. To enable features to “tolerate” `servlet-3.1`, modify the feature manifest as follows:

```
Subsystem-Content: com.ibm.websphere.appserver.servlet-3.0; ibm.tolerates:="3.1"; type="osgi.subsystem.feature"
```

If your server configuration includes multiple versions of a singleton feature, either through direct configuration in the `server.xml` file, or through feature dependencies, that configuration is in error and neither version of that feature is loaded. This error results in a message similar to the following:

```
[ERROR ] CWWKF0033E: The singleton features servlet-3.1 and servlet-3.0 cannot be loaded at the same time. The configured
```

To resolve this problem, ensure that the configured features all specify, or tolerate, the same version of that singleton feature. If you have hard requirements on both feature versions, you must move some of your applications to a different server. For more information on tolerating singleton features, see [Tolerating singleton features](#).

8.5.5.0

### Superseded features

The **superseded** label on a feature indicates that a new feature or a combination of features might provide an advantage over using the superseded feature. For example, new, finer-grained features might be used in place of the superseded one in order to reduce the server footprint by excluding content that might not be necessary. The new feature or features might not completely replace the function of the superseded feature, so you must consider your scenario before deciding whether to change your

configuration. Superseded features remain completely supported and valid for use in your configuration; the **superseded** label just provides an indication that you might be able to improve your configuration.

**8.5.5.0** Very occasionally, a feature that includes other features is superseded by a new version of the feature that does not include all those features; the features that are not included in the new version are considered to be *separated*. If your application needs to use the functions of a separated feature, you must explicitly add the separated feature to your configuration.

For example, featureA and featureB have the following conditions:

- featureA-1.0 includes featureB-1.0
- featureA-2.0 does not include featureB-1.0 (or any later versions of featureB)

If your application uses featureB functions, either of these configurations will work:

- Include featureA-1.0 in your server.xml file
- Include featureA-2.0 and featureB-1.0 in your server.xml file

## Liberty features

Features are the units of functionality by which you control the pieces of the runtime environment that are loaded into a particular server.

The following table lists the Liberty features that are supported for each WebSphere Application Server Liberty edition.

**Tip:** To install all features that apply your Liberty edition, you can install a feature bundle add-on. WebSphere Application Server Network Deployment Liberty has two bundles: The `ndMemberBundle` add-on contains most features and is for servers that are clustered and auto-scaled in a Liberty collective, and the `ndControllerBundle` add-on contains a small set of features only for managing Liberty collectives.

Table 6. Liberty features supported for each WebSphere Application Server Liberty edition

Liberty feature	WebSphere Application Server Liberty Core	WebSphere Application Server and WebSphere Application Server - Express®	WebSphere Application Server Network Deployment (Distributed operating systems and IBM i)	WebSphere Application Server for z/OS
<b>Feature bundle add-on</b>	<code>libertyCoreBundle</code>	<code>baseBundle</code>	<code>ndMemberBundle</code> : All except controller features  <code>ndControllerBundle</code> : Only features marked with <sup>1</sup>	<code>zosBundle</code>
<b>Java EE 7 Web Profile</b>				
<b>8.5.5.6</b> <code>beanValidation-1.1</code>	✓	✓	✓	✓
<b>8.5.5.6</b> <code>cdi-1.2</code>	✓	✓	✓	✓
<b>8.5.5.6</b> <code>ejbLite-3.2</code>	✓	✓	✓	✓
<code>el-3.0</code>	✓	✓	✓	✓
<b>8.5.5.6</b> <code>jaxrs-2.0</code>	✓	✓	✓	✓

Table 6. Liberty features supported for each WebSphere Application Server Liberty edition (continued)

Liberty feature	WebSphere Application Server Liberty Core	WebSphere Application Server and WebSphere Application Server - Express®	WebSphere Application Server Network Deployment (Distributed operating systems and IBM i)	WebSphere Application Server for z/OS
8.5.5.6 jaxrsClient-2.0	✓	✓	✓	✓
jdbc-4.1	✓	✓	✓	✓
jndi-1.0	✓	✓	✓	✓
8.5.5.6 jpa-2.1	✓	✓	✓	✓
8.5.5.6 jsf-2.2	✓	✓	✓	✓
jsonp-1.0	✓	✓	✓	✓
jsp-2.3	✓	✓	✓	✓
managedBeans-1.0	✓	✓	✓	✓
servlet-3.1	✓	✓	✓	✓
8.5.5.6 webProfile-7.0	✓	✓	✓	✓
websocket-1.0	✓	✓	✓	✓
websocket-1.1	✓	✓	✓	✓
<b>Java EE 7 Full Platform</b>				
8.5.5.6 appClientSupport-1.0		✓	✓	✓
8.5.5.6 appSecurityClient-1.0		✓	✓	✓
8.5.5.6 batch-1.0		✓	✓	✓
concurrent-1.0	✓	✓	✓	✓
8.5.5.6 ejb-3.2		✓	✓	✓
8.5.5.6 ejbHome-3.2		✓	✓	✓
8.5.5.6 ejbPersistentTimer-3.2		✓	✓	✓
8.5.5.6 ejbRemote-3.2		✓	✓	✓
8.5.5.6 j2eeManagement-1.1		✓	✓	✓
8.5.5.6 jacc-1.5	✓	✓	✓	✓
8.5.5.6 jaspic-1.1	✓	✓	✓	✓
8.5.5.6 javaee-7.0		✓	✓	✓
8.5.5.6 javaeeClient-7.0		✓	✓	✓
8.5.5.6 javaMail-1.5	✓	✓	✓	✓
jaxb-2.2		✓	✓	✓
jaxws-2.2		✓	✓	✓
8.5.5.6 jca-1.7		✓	✓	✓

Table 6. Liberty features supported for each WebSphere Application Server Liberty edition (continued)

Liberty feature	WebSphere Application Server Liberty Core	WebSphere Application Server and WebSphere Application Server - Express®	WebSphere Application Server Network Deployment (Distributed operating systems and IBM i)	WebSphere Application Server for z/OS
jcaInboundSecurity-1.0		✓	✓	✓
8.5.5.6 jms-2.0		✓	✓	✓
8.5.5.6 jmsMdb-3.2		✓	✓	✓
8.5.5.6 mdb-3.2		✓	✓	✓
8.5.5.6 wasJmsClient-2.0		✓	✓	✓
wasJmsSecurity-1.0		✓	✓	✓
wasJmsServer-1.0		✓	✓	✓
<b>Extended Programming Models</b>				
cloudant-1.0		✓	✓	✓
couchdb-1.0		✓	✓	✓
distributedMap-1.0	✓	✓	✓	✓
json-1.0	✓	✓	✓	✓
mongodb-2.0		✓	✓	✓
8.5.5.7 rtcomm-1.0		✓	✓	✓
8.5.5.7 rtcommGateway-1.0		✓	✓	✓
8.5.5.7 sipServlet-1.1		✓	✓	✓
<b>Enterprise OSGi</b>				
blueprint-1.0	✓	✓	✓	✓
osgiAppIntegration-1.0	✓	✓	✓	✓
8.5.5.9 osgiBundle-1.0	✓	✓	✓	✓
osgi.jpaa-1.0	✓	✓	✓	✓
wab-1.0	✓	✓	✓	✓
<b>Operations</b>				
8.5.5.8 apiDiscovery-1.0	✓	✓	✓	✓
appSecurity-1.0	✓	✓	✓	✓
appSecurity-2.0	✓	✓	✓	✓
8.5.5.6 batchManagement-1.0		✓	✓	✓
8.5.5.7 bells-1.0	✓	✓	✓	✓
8.5.5.9 bluemixUtility-1.0	✓	✓	✓	✓

Table 6. Liberty features supported for each WebSphere Application Server Liberty edition (continued)

Liberty feature	WebSphere Application Server Liberty Core	WebSphere Application Server and WebSphere Application Server - Express®	WebSphere Application Server Network Deployment (Distributed operating systems and IBM i)	WebSphere Application Server for z/OS
8.5.5.6 eventLogging-1.0	✓	✓	✓	✓
ldapRegistry-3.0	✓	✓	✓	✓
localConnector-1.0	✓	✓	✓	✓
8.5.5.9 logstashCollector-1.0	✓	✓	✓	✓
monitor-1.0	✓	✓	✓	✓
oauth-2.0	✓	✓	✓	✓
openid-2.0	✓	✓	✓	✓
openidConnectClient-1.0	✓	✓	✓	✓
openidConnectServer-1.0	✓	✓	✓	✓
osgiConsole-1.0	✓	✓	✓	✓
8.5.5.9 passwordUtilities-1.0		✓	✓	✓
8.5.5.6 requestTiming-1.0	✓	✓	✓	✓
restConnector-1.0	✓	✓	✓	✓
8.5.5.7 samlWeb-2.0	✓	✓	✓	✓
serverStatus-1.0	✓	✓	✓	✓
sessionDatabase-1.0	✓	✓	✓	✓
spnego-1.0	✓	✓	✓	✓
ssl-1.0	✓	✓	✓	✓
timedOperations-1.0	✓	✓	✓	✓
webCache-1.0	✓	✓	✓	✓
8.5.5.6 wmqJmsClient-2.0		✓	✓	✓
wsSecurity-1.1		✓	✓	✓
8.5.5.9 wsAtomicTransaction-1.2		✓	✓	✓
<b>Systems Management</b>				
adminCenter-1.0	✓	✓	✓ <sup>1</sup>	✓
clusterMember-1.0			✓	✓
collectiveController-1.0			✓ <sup>1</sup>	✓
collectiveMember-1.0	✓	✓	✓	✓
dynamicRouting-1.0			✓ <sup>1</sup>	✓
8.5.5.7 healthAnalyzer-1.0			✓	✓
8.5.5.7 healthManager-1.0			✓ <sup>1</sup>	✓

Table 6. Liberty features supported for each WebSphere Application Server Liberty edition (continued)

Liberty feature	WebSphere Application Server Liberty Core	WebSphere Application Server and WebSphere Application Server - Express®	WebSphere Application Server Network Deployment (Distributed operating systems and IBM i)	WebSphere Application Server for z/OS
scalingController-1.0			✓ <sup>1</sup>	✓
scalingMember-1.0			✓	✓
<b>z/OS</b>				
zosConnect-1.0				✓
8.5.5.7 zosConnect-1.2				✓
zosLocalAdapters-1.0				✓
zosSecurity-1.0				✓
zosTransaction-1.0				✓
zosWlm-1.0				✓
<b>Java EE 6 Web Profile</b>				
beanValidation-1.0	✓	✓	✓	✓
cdi-1.0	✓	✓	✓	✓
ejbLite-3.1	✓	✓	✓	✓
jdbc-4.0	✓	✓	✓	✓
jndi-1.0	✓	✓	✓	✓
jpa-2.0	✓	✓	✓	✓
jsf-2.0	✓	✓	✓	✓
jsp-2.2	✓	✓	✓	✓
servlet-3.0	✓	✓	✓	✓
webProfile-6.0	✓	✓	✓	✓
<b>Java EE 6 Technologies</b>				
jaxb-2.2		✓	✓	✓
jaxrs-1.1	✓	✓	✓	✓
jaxws-2.2		✓	✓	✓
jca-1.6		✓	✓	✓
jcaInboundSecurity-1.0		✓	✓	✓
jms-1.1		✓	✓	✓
jmsMdb-3.1		✓	✓	✓
mdb-3.1		✓	✓	✓
wasJmsClient-1.1		✓	✓	✓
wasJmsSecurity-1.0		✓	✓	✓

Table 6. Liberty features supported for each WebSphere Application Server Liberty edition (continued)

Liberty feature	WebSphere Application Server Liberty Core	WebSphere Application Server and WebSphere Application Server - Express®	WebSphere Application Server Network Deployment (Distributed operating systems and IBM i)	WebSphere Application Server for z/OS
wasJmsServer-1.0		✓	✓	✓
wmqJmsClient-1.1		✓	✓	✓

## Feature descriptions

The following list contains information about the features you can add to your server configuration. Including a feature in the configuration might cause one or more additional features to be loaded automatically. For example, if you include the `wab-1.0` feature, the `servlet-3.0` and `blueprint-1.0` features are loaded automatically. Each feature includes a brief description, and an example of how the feature is declared within the `<featureManager>` element inside the `server.xml` file. For example:

```
<server>
  <featureManager>
    <feature>servlet-3.0</feature>
    <feature>localConnector-1.0</feature>
  </featureManager>
</server>
```

### Java EE 7 Web Profile

#### 8.5.5.6 Bean validation

```
<feature>beanValidation-1.1</feature>
```

The `beanValidation-1.1` feature provides validations for JavaBeans at each layer of an application. The validation can be applied to all layers of JavaBeans in an application by using annotations or a `validation.xml` deployment descriptor.

See “Bean validation feature restrictions” on page 2337.

For `beanValidation-1.1` feature configuration information, see “Bean Validation 1.1” on page 863.

#### 8.5.5.6 CDI

```
<feature>cdi-1.2</feature>
```

The `cdi-1.2` feature enables support for the Contexts and Dependency Injection 1.2 specification on Liberty.

See “Administering Contexts and Dependency Injection applications on Liberty” on page 1725.

For `cdi-1.2` feature configuration information, see “Contexts and Dependency Injection 1.2” on page 868.

### Enterprise Java Beans (EJB) Lite

```
8.5.5.6 <feature>ejbLite-3.2</feature>
```

The `ejbLite-3.2` feature provides support for EJB applications that are written to the EJB Lite subset of the EJB 3.2 specification.

Note that the EJB 3.2 Lite API Group does not include the embeddable EJB container, and the product does not provide an EJB 3.2 embeddable container.

Also, the following features are not compatible with the `ejbLite-3.2` feature:

- `cdi-1.0`
- `jmsMdb-3.1`
- `mdb-3.1`

See “Developing EJB applications on Liberty” on page 2116.

For `ejbLite-3.2` feature configuration information, see “Enterprise JavaBeans Lite 3.2” on page 875.

### Expression Language 3.0

```
<feature>el-3.0</feature>
```

This feature enables support for the Expression Language (EL) 3.0.

See “Configuring Liberty for Expression Language 3.0” on page 1721.

For `el-3.0` feature configuration information, see “Expression Language 3.0” on page 878.

#### 8.5.5.6 Java API for RESTful Web Services (JAX-RS)

```
<feature>jaxrs-2.0</feature>
```

The `jaxrs-2.0` feature provides support for the Java API for RESTful Web Services on Liberty.

See “Configuring JAX-RS 2.0 client” on page 2162 and “JAX-RS 2.0 integration with EJB and CDI” on page 2171.

For `jaxrs-2.0` feature configuration information, see “Java RESTful Services 2.0” on page 914.

#### 8.5.5.6 Java EE Client API for JAX-RS 2.0

```
<feature>jaxrsClient-2.0</feature>
```

The `jaxrsClient-2.0` feature provides support for Java Client API for JAX-RS 2.0

See “Configuring JAX-RS 2.0 client” on page 2162 and “JAX-RS 2.0 integration with EJB and CDI” on page 2171.

For `jaxrsClient-2.0` feature configuration information, see “Java RESTful Services Client 2.0” on page 914.

### Java Database Connectivity (JDBC)

```
<feature>jdbc-4.1</feature>
```

You can take an existing application that uses Java Database Connectivity (JDBC) and a data source, and deploy the application to a server. The `jdbc-4.1` feature provides support for applications that access a database.

See “Configuring relational database connectivity in Liberty” on page 1672.

For `jdbc-4.1` feature configuration information, see “Java Database Connectivity 4.1” on page 895.

### Java Naming and Directory Interface (JNDI)

```
<feature>jndi-1.0</feature>
```

The `jndi-1.0` feature provides support for a single JNDI entry definition in the server configuration of Liberty.

See “Developing with the JNDI default namespace in a Liberty feature” on page 1819.

For `jndi-1.0` feature configuration information, see “Java Naming and Directory Interface” on page 902.

#### 8.5.5.6 **Java Persistence API 2.1**

`<feature>jpa-2.1</feature>`

The `jpa-2.1` feature provides support for applications that use application-managed and container-managed JPA written to the JPA 2.1 specification and is backed by EclipseLink.

See “Java Persistence API (JPA) feature overview” on page 1016.

For `jpa-2.1` feature configuration information, see “Java Persistence API 2.1” on page 906.

#### 8.5.5.6 **JavaServer Faces (JSF)**

`<feature>jsf-2.2</feature>`

This feature enables support for web applications that use the Java Server Faces (JSF) 2.2 framework. This framework simplifies the construction of user interfaces.

See “Configuring Liberty for JavaServer Faces 2.2” on page 1722.

For `jsf-2.2` feature configuration information, see “JavaServer Faces 2.2” on page 927.

### **JavaScript Object Notation Processing**

`<feature>jsonp-1.0</feature>`

The Java API for JSON Processing (JSON-P) feature provides a standardized method for constructing and manipulating data to be rendered in JavaScript Object Notation (JSON).

For `jsonp-1.0` feature configuration information, see “JavaScript Object Notation Processing” on page 924.

### **JavaServer Pages (JSP)**

`<feature>jsp-2.3</feature>`

This feature enables support for Java Server Pages (JSPs) that are written to the JSP 2.3 specification. This framework simplifies the construction of user interfaces. Enabling this feature also enables the Expression Language (EL) version 3.0 feature. `el-3.0`.

See “Configuring Liberty for JavaServer Pages 2.3” on page 1724.

For `jsp-2.3` feature configuration information, see “JavaServer Pages 2.3” on page 928.

### **Managed Beans**

`<feature>managedBeans-1.0</feature>`

The `managedBeans-1.0` feature provides support for the Managed Beans 1.0 specification (JSR-316). This feature enables use of the `javax.annotation.ManagedBean` annotation.

For `managedBeans-1.0` feature configuration information, see “Java EE Managed Bean 1.0” on page 897.

### **Servlet 3.1**

`<feature>servlet-3.1</feature>`

The `servlet-3.1` feature enables support for HTTP Servlets that are written to the Java Servlet 3.1 specification.

See “Configuring Liberty for Servlet 3.1” on page 1713 and “Servlet 3.1 behavior changes” on page 1714.

For `servlet-3.1` feature configuration information, see “Java Servlets 3.1” on page 917.

#### 8.5.5.6 **Web Profile 7.0**

`<feature>webProfile-7.0</feature>`

This feature provides a convenient combination of the Liberty features that are required to support the Java EE 7 Web Profile.

See “Java EE 7 in Liberty” on page 4.

For webProfile-7.0 feature configuration information, see “Java EE Web Profile 7.0” on page 899.

## WebSocket

```
<feature>websocket-1.0</feature>
```

```
<feature>websocket-1.1</feature>
```

WebSocket is a standard protocol that enables a web browser or client application and a web server application to communicate by using one full duplex connection.

See Liberty: WebSocket and “Developing WebSocket applications in Liberty” on page 2137.

For websocket-1.0 feature configuration information, see “Java WebSocket 1.0” on page 921.

For websocket-1.1 feature configuration information, see “Java WebSocket 1.1” on page 922.

## Java EE 7 Full Platform

### 8.5.5.6 Application Client Support

```
<feature>appClientSupport-1.0</feature>
```

The appClientSupport-1.0 feature enables the server to process Java EE metadata inside the client module of an application, for example, read the deployment descriptor XML file and/or annotations and make them available to other modules in the application if necessary. It also enables the remote application client process to communicate with the server to do JNDI lookups.

The appClientSupport-1.0 feature is enabled in the server.xml file only.

For appClientSupport-1.0 feature configuration information, see “Application Client Support for Server” on page 856.

### 8.5.5.6 Application Client Container Security

```
<feature>appSecurityClient-1.0</feature>
```

To enable security on the client container, add the appSecurityClient-1.0 feature to your client.xml file.

The appSecurityClient-1.0 feature enables SSL, CSIV2, and JAAS on the client. You must configure SSL to ensure communications between the client and server are secure and encrypted.

See “Security on the Liberty application client container” on page 1001 and “Configuring security for the Liberty application client container and its applications” on page 1984.

For appSecurityClient-1.0 feature configuration information, see “Application Security for Client 1.0” on page 858.

### 8.5.5.6 Batch

```
<feature>batch-1.0</feature>
```

The batch-1.0 feature enables the use of the JSR-352 programming model.

See “Java batch and managed batch overview” on page 2208.

For batch-1.0 feature configuration information, see “Batch API 1.0” on page 860.

## Managed Executors and Thread Factories

```
<feature>concurrent-1.0</feature>
```

The concurrent-1.0 feature enables the creation of managed executor services that allow applications to submit tasks to run concurrently, with thread context that is managed by

the application server. The feature also enables the creation of managed thread factories to create threads that run with the thread context of the component that looks up the managed thread factory.

See “Configuring managed scheduled executors” on page 1637.

For concurrent-1.0 feature configuration information, see “Concurrency Utilities for Java EE 1.0” on page 866.

## Enterprise Java Beans (EJB)

**8.5.5.6** <feature>ejb-3.2</feature>

The `ejb-3.2` feature provides support for EJB applications that are written to the EJB 3.2 specification.

This feature includes the following features:

- **8.5.5.6** <feature>ejbLite-3.2</feature>

This feature gives support for EJB applications that are written to the EJB Lite subset of the EJB 3.2 specification. For `ejbLite-3.2` feature configuration information, see “Enterprise JavaBeans Lite 3.2” on page 875.

- **8.5.5.6** <feature>ejbHome-3.2</feature>

This feature gives support for the EJB 2.x APIs. For `ejbHome-3.2` feature configuration information, see “Enterprise JavaBeans Home Interfaces 3.2” on page 873.

- **8.5.5.6** <feature>ejbPersistentTimer-3.2</feature>

This feature gives support for persistent EJB timers. For `ejbPersistentTimer-3.2` feature configuration information, see “Enterprise JavaBeans Persistent Timers 3.2” on page 876.

- **8.5.5.6** <feature>ejbRemote-3.2</feature>

This feature gives support for remote EJB interfaces. For `ejbRemote-3.2` feature configuration information, see “Enterprise JavaBeans Remote 3.2” on page 876.

- **8.5.5.6** <feature>mdb-3.2</feature>

This feature gives support for message-driven beans. For `mdb-3.2` feature configuration information, see “Message-Driven Beans 3.2” on page 935.

The `mdb-3.2` feature supersedes the `jmsMdb-3.2` feature. For information about the `jmsMdb-3.2` feature, see “Deploying message-driven beans to connect to WebSphere MQ” on page 2201.

If full EJB 3.2 support is not required, various combinations of these features can be used to provide the support that you need.

See “Developing EJB applications on Liberty” on page 2116.

For `ejb-3.2` feature configuration information, see “Enterprise JavaBeans 3.2” on page 873.

### **8.5.5.6** J2EE Management 1.1

<feature>j2eeManagement-1.1</feature>

The `j2eeManagement-1.1` feature provides standard interfaces to manageable aspects of Java EE 7 and enables applications to use the interfaces defined in the JSR 77 specification.

To invoke Management EJB APIs, the server configuration must have both the `j2eeManagement-1.1` and `ejbRemote-3.2` features in a feature manager. After both features are in the server configuration, you can invoke Management EJB API through JNDI name lookup. The Management EJB binding name (JNDI lookup name) is `ejb/mejb/MEJB`.

See “j2eeManagement-1.1 feature restrictions” on page 2338.

For `j2eeManagement-1.1` feature configuration information, see “J2EE Management 1.1” on page 880.

#### 8.5.5.6 **Java Authorization Contract for Containers 1.5**

```
<feature>jacc-1.5</feature>
```

The jacc-1.5 feature enables support for Java Authorization Contract for Containers (JACC) version 1.5. In order to add the jacc-1.5 feature to your server, you need to add the third party JACC provider which is not a part of the WebSphere Application Server Liberty.

See “Developing a Java Authorization Contract for Containers (JACC) Authorization Provider” on page 2009.

For jacc-1.5 feature configuration information, see “Java Authorization Contract for Containers 1.5” on page 891.

#### 8.5.5.6 **Java Authentication SPI for Containers 1.1**

```
<feature>jaspic-1.1</feature>
```

The jaspic-1.1 feature enables support for securing the server runtime environment and applications using Java Authentication SPI for Containers (JASPIC) providers as defined in JSR-196.

See “Configuring a Java Authentication SPI for Containers (JASPIC) User Feature” on page 1871.

For jaspic-1.1 feature configuration information, see “Java Authentication SPI for Containers 1.1” on page 890.

#### 8.5.5.6 **Java EE**

```
<feature>javaee-7.0</feature>
```

This feature provides a convenient combination of the Liberty features that are required to support the Java EE 7.0 Full Platform.

See “Java EE 7 in Liberty” on page 4.

For javaee-7.0 feature configuration information, see “Java EE Full Platform 7.0” on page 896.

#### 8.5.5.6 **Java EE Application Client 7.0**

```
<feature>javaeeClient-7.0</feature>
```

This feature enables support for Java EE Application Client 7.0.

See “Creating a Liberty application client manually” on page 1446.

For javaeeClient-7.0 feature configuration information, see “Java EE V7 Application Client” on page 898.

#### 8.5.5.6 **JavaMail API**

```
<feature>javaMail-1.5</feature>
```

The JavaMail API supports communication between external mail servers and Liberty applications. See “Administering JavaMail on Liberty” on page 1730.

For javaMail-1.5 feature configuration information, see “JavaMail 1.5” on page 923.

#### **Java Architecture for XML Binding (JAXB)**

```
<feature>jaxb-2.2</feature>
```

The jaxb-2.2 feature provides support for the Java Architecture for XML Binding (JAXB) on Liberty.

See JAXB and “jaxb-2.2 feature restriction” on page 2338.

For jaxb-2.2 feature configuration information, see “Java XML Bindings 2.2” on page 922.

#### **Java API for XML-Based Web Services (JAX-WS)**

```
<feature>jaxws-2.2</feature>
```

The jaxws-2.2 feature provides support for the Java API for XML-Based Web Services on Liberty.

- For web applications that support the JAX-WS programming model, you must enable the servlet-3.0 and jaxws-2.2 server features in the server.xml file.
- For EJB applications that support the JAX-WS programming model, you must enable the ejbLite-3.1, servlet-3.0, and jaxws-2.2 server features in the server.xml file.
- For applications that use the global handler services, you must enable the jaxrs-1.1 or the jaxws-2.2 feature in the server.xml file.

See “Deploying JAX-WS applications to Liberty” on page 2178 and “jaxws-2.2 feature restrictions” on page 2339.

For jaxws-2.2 feature configuration information, see “Java Web Services 2.2” on page 920.

#### 8.5.5.6 **Java EE Connector Architecture 1.7**

```
<feature>jca-1.7</feature>
```

The jca-1.7 feature provides configuration elements to define instances of connection factories, administered objects, and activation specifications, and to associate these instances with an installed resource adapter.

For jca-1.7 feature configuration information, see “Java Connector Architecture 1.7” on page 893.

#### **Java EE Connector Architecture Inbound Security**

```
<feature>jcaInboundSecurity-1.0</feature>
```

The jcaInboundSecurity-1.0 feature enables security inflow for resource adapters.

For jcaInboundSecurity-1.0 feature configuration information, see “Java Connector Architecture 1.0 Security Inflow” on page 891.

#### 8.5.5.6 **Java Message Service 2.0**

```
<feature>jms-2.0</feature>
```

The jms-2.0 feature enables the configuration of resource adapters to access messaging systems using the Java Message Service API. This also includes the configuration JMS connection factories, queues, topics and activation specifications. Any JMS resource adapter that complies with the JCA 1.6 specification can be used.

See “Enabling JMS messaging for Liberty” on page 1121 and “Deploying messaging applications to Liberty” on page 2195.

For jms-2.0 feature configuration information, see Java Messaging Service 2.0.

#### **Embedded Liberty Messaging features**

```
8.5.5.6 <feature>wasJmsClient-2.0</feature>
```

The wasJmsClient-2.0 feature supersedes the wasJmsClient-1.1 feature. The wasJmsClient-2.0 feature is compliant with the JMS 2.0 specification and is supported only on IBM JDK 7 or later.

See “Enabling JMS messaging for Liberty” on page 1121 and “Deploying messaging applications to Liberty” on page 2195.

For wasJmsClient-2.0 feature configuration information, see “JMS 2.0 Client for Message Server” on page 884.

```
<feature>wasJmsSecurity-1.0</feature>
```

The wasJmsSecurity-1.0 feature supports secure connections to the messaging engine. When the wasJmsSecurity-1.0 feature is enabled, it starts authenticating and authorizing the users who are trying to connect to the messaging engine. The user is authenticated against the registry that is defined in the server.xml file. When the user wants to access a

destination such as a topic or a queue, then the user must be granted the required permissions. The access to the destination is defined in the `<messagingSecurity>` element (the child element of the `messagingEngine` element) in the `server.xml` file. If the `wasJmsSecurity-1.0` feature is added and the `<messagingSecurity>` element is not defined in the `server.xml` file, then the users cannot connect to the messaging engine or perform any messaging action (for example, sending or receiving messages from the destinations). For `wasJmsSecurity-1.0` feature configuration information, see “Message Server Security 1.0” on page 933.

**Notes:**

- Configuring the user registry is a prerequisite for the `wasJmsSecurity-1.0` feature. Ensure that a user registry is configured before the `wasJmsSecurity-1.0` feature is enabled.
- When you enable the `wasJmsSecurity-1.0` feature, you must also configure the `<messagingSecurity>` element, which is the child element of the `<messagingEngine>` element, in the `server.xml` file. This configuration enables authorized users to access messaging destinations.

```
<feature>wasJmsServer-1.0</feature>
```

The `wasJmsServer-1.0` feature enables the JMS messaging engine run time to be initialized. The messaging run time is responsible for providing the application connectivity, managing the state of destinations such as topics or queues, and handling quality of service, security, and transactions. This feature also provides support for the inbound connections from the remote messaging applications. The remote messaging applications can connect to the JMS messaging engine through TCP/IP over SSL or non-SSL.

To connect using SSL, you must enable the SSL feature.

See “Enabling secure JMS messaging for Liberty” on page 1126.

For `wasJmsServer-1.0` feature configuration information, see “Message Server 1.0” on page 932.

## Extended Programming Models

### 8.5.5.9 Cloudant integration

```
<feature>cloudant-1.0</feature>
```

This feature enables connections to Cloudant by providing a connector instance configured in the server configuration. The connector instance can be injected or accessed through JNDI. Applications use the Cloudant client library to use the connector instance.

For `cloudant-1.0` feature configuration information, see “Cloudant Integration 1.0” on page 864.

### CouchDB

```
<feature>couchdb-1.0</feature>
```

The `couchdb-1.0` feature provides support for CouchDB instances and associated database connections. Access to CouchDB connections is available either by JNDI lookup or resource injection.

See “Configuring CouchDB connectivity with the ektorp client library in Liberty” on page 1686.

For `couchdb-1.0` feature configuration information, see “CouchDB Integration 1.0” on page 869.

### Cache Service

```
<feature>distributedMap-1.0</feature>
```

This feature provides a local cache service that can be accessed by using the DistributedMap API. A default cache is bound in JNDI at services/cache/distributedmap. You can distribute a cache by adding a network cache provider such as WebSphere eXtreme Scale.

For distributedMap-1.0 feature configuration information, see “Distributed Map interface for Dynamic Caching” on page 870.

### JavaScript Object Notation (JSON4J) Library

```
<feature>json-1.0</feature>
```

The json-1.0 feature provides access to the JSON4J library that provides a set of JSON handling classes for Java environments. The JSON4J library provides a simple Java model for constructing and manipulating data to be rendered as JSON data.

See Using JSON content in JAX-RS application requests and responses and JSON4J Libraries API.

For json-1.0 feature configuration information, see “JavaScript Object Notation for Java” on page 924.

### MongoDB

```
<feature>mongodb-2.0</feature>
```

The mongodb-2.0 feature provides support for MongoDB instances and associated database connections. Access to MongoDB connections is available either by JNDI lookup or resource injection. The native com.mongodb API performs the database manipulation.

See “Configuring MongoDB connectivity in Liberty” on page 1683.

For mongodb-2.0 feature configuration information, see “MongoDB Integration 2.0” on page 936.

#### 8.5.5.7 Real-Time Communications

```
<feature>rtcomm-1.0</feature>
```

The Liberty Real-Time Communications feature enables a highly-scalable call signalling engine that can be used to connect WebRTC clients into real-time audio/video/data calls. The feature supports both registration of clients as well as the exchange of signalling needed to create a WebRTC peer connection between two endpoints.

For rtcomm-1.0 feature configuration information, see “Real-Time Communications” on page 947.

#### 8.5.5.7 RTComm Gateway

```
<feature>rtcommGateway-1.0</feature>
```

The rtcommGateway-1.0 feature adds the capability for connecting Session Initiation Protocol (SIP) with RTComm WebRTC endpoints for the exchange of audio and video streams.

For rtcommGateway-1.0 feature configuration information, see “WebRTC Rtcomm Gateway” on page 958.

#### 8.5.5.7 SIP Servlet

```
<feature>sipServlet-1.1</feature>
```

The sipServlet-1.1 feature provides support for SIP Servlet Specification 1.1, also known as JSR 289. Session Initiation Protocol (SIP) is a control protocol for many interactive services, including audio, video, and peer-to-peer communication.

See “Liberty: Session Initiation Protocol (SIP)” on page 1033 and “Administering Session Initiation Protocol (SIP) on Liberty” on page 1728.

For sipServlet-1.1 feature configuration information, see “SIP Servlet” on page 949.

## Enterprise OSGi

## Blueprint

```
<feature>blueprint-1.0</feature>
```

The `blueprint-1.0` feature enables support for deploying OSGi applications that use the OSGi blueprint container specification. With the OSGi Applications support in WebSphere Application Server, you can develop and deploy modular applications that use Java EE and OSGi technologies.

See “Locating OSGi applications” on page 1818 and OSGi Applications.

For `blueprint-1.0` feature configuration information, see “OSGi Blueprint” on page 938.

## OSGi application integration

```
<feature>osgiAppIntegration-1.0</feature>
```

Use the `osgiAppIntegration-1.0` feature to enable the OSGi applications that are available within the same Java virtual machine to share their services with each other.

For more information about `Application-ImportService` and `Application-ExportService` headers, see Application manifest files.

For `osgiAppIntegration-1.0` feature configuration information, see “OSGi Application Integration” on page 938.

### 8.5.5.9 OSGi bundle

```
<feature>osgiBundle-1.0</feature>
```

This feature enables support for deploying OSGi applications. With the OSGi Applications support, you can develop and deploy modular applications that use Java EE and OSGi technologies.

For `osgiBundle-1.0` feature configuration information, see `osgiBundle-1.0`.

## OSGi JPA

```
<feature>osgi.jpa-1.0</feature>
```

The `osgi.jpa-1.0` feature provides JPA support for OSGi applications on Liberty.

See “Deploying OSGi applications to Liberty” on page 2149.

For `osgi.jpa-1.0` feature configuration information, see “OSGi Java Persistence API” on page 942.

## Web application bundle (WAB)

```
<feature>wab-1.0</feature>
```

This feature enables support for warnings to be logged when certain operations in the application server are running more slowly than expected. The `wab-1.0` feature provides support for WABs that are inside enterprise bundles. The `wab-1.0` feature provides support for WABs that are inside enterprise bundles.

This feature supports the following resources packaged inside a WAB:

- Static web content and JSPs.
- HTTP servlets written to the Servlet 3.0 specification.
- Blueprint applications.

If you include the `wab-1.0` feature, you also include the `servlet-3.0` and `blueprint-1.0` features.

See “Deploying OSGi applications to Liberty” on page 2149.

For `wab-1.0` feature configuration information, see “OSGi Web Application Bundles” on page 943.

## Operations

### 8.5.5.8

## API Discovery

```
<feature>apiDiscovery-1.0</feature>
```

The `apiDiscovery-1.0` feature enables you to discover your REST API documentation. Use the feature to find REST APIs that are available on a Liberty server and then use the Swagger user interface to invoke the found REST endpoints. See “Discovering REST API documentation on a Liberty server” on page 2260.

## Security

```
<feature>appSecurity-2.0</feature>
```

This version of the `appSecurity` feature provides only certain aspects of security, based explicitly on the presence of other features. Additionally, it does not automatically include the `servlet-3.0` or `ldapRegistry-3.0` features, thereby reducing the server footprint. To secure web applications, you must include the `servlet-3.0` feature. To enable EJB security, you must include the `ejbLite-3.1` feature. To support an LDAP user registry, you must include the `ldapRegistry-3.0` feature.

### Note:

- The `appSecurity-2.0` feature supersedes `appSecurity-1.0`. The features are the same except that `appSecurity-2.0` does not automatically include `servlet-3.0` or `ldapRegistry-3.0`. You can choose to use the `appSecurity-2.0` version instead in your server configuration. See “Superseded features” on page 825.
  - To enable web security, you must specify the `servlet-3.0` feature in the `server.xml` file.
  - To enable support for LDAP, you must specify the `ldapRegistry-3.0` feature in the `server.xml` file.

The `appSecurity-1.0` and `appSecurity-2.0` features provide support for securing the server runtime environment and applications. The following aspects are supported:

- Basic user registry
- Lightweight Directory Access Protocol (LDAP) user registry
- Basic authorization
- Web application security
  - Basic authentication login
  - Form-login Form-logout
  - Programmatic APIs: `getRemoteUser`, `getUserPrincipal`, `isUserInRole`, `authenticate`, `logout`, and `login`.
- **8.5.5.0** EJB application security
  - All security annotations and all security elements that can be specified in the `ejb-jar.xml` file.
  - Programmatic APIs: `getCallerPrincipal`, `isCallerInRole`, and `getCallerIdentity`. The `getCallerIdentity` API is not supported for Singleton session beans.
  - EJB extension settings in the `ibm-ejb-jar-ext.xml` file for **run-as-mode** of `CALLER_IDENTITY` and `SPECIFIED_IDENTITY` (`SYSTEM_IDENTITY` is not supported).

When you add the `appSecurity-1.0` or `appSecurity-2.0` feature to your server, you must also configure a user registry, such as the basic user registry or the LDAP user registry.

See Chapter 8, “Securing Liberty and its applications,” on page 1829 and “`appSecurity-2.0` feature restrictions” on page 2335..

For `appSecurity-1.0` feature configuration information, see “Application Security 1.0” on page 857

page 857.

For appSecurity-2.0 feature configuration information, see “Application Security 2.0” on page 857.

#### 8.5.5.6 **Managed Batch**

```
<feature>batchManagement-1.0</feature>
```

The batchManagement-1.0 feature provides a REST interface for remote job submission and the batchManager command-line client utility.

See “Java batch and managed batch overview” on page 2208

For batchManagement-1.0 feature configuration information, see “Batch Management” on page 861.

#### 8.5.5.7 **Basic Extensions using Liberty Libraries (BELL)**

```
<feature>bells-1.0</feature>
```

This feature enables the configuration of Basic Extensions using Liberty Libraries (BELL). Use this feature to extend some parts of the server runtime using libraries, rather than using Liberty features. BELL uses the Java Service Loader pattern to provide the implementation class name.

For bells-1.0 feature configuration information, see “Basic Extensions using Liberty Libraries” on page 859.

#### 8.5.5.9 **Bluemix Utility**

```
<feature>bluemixUtility-1.0</feature>
```

This feature makes it easier to configure access to IBM Bluemix managed services. See “Setting up a Liberty server to use Bluemix services” on page 1529.

For bluemixUtility-1.0 feature configuration information, see bluemixUtility-1.0.

#### 8.5.5.6 **Event Logging**

```
<feature>eventLogging-1.0</feature>
```

The eventLogging-1.0 feature logs a record of events, such as the JDBC requests and servlet requests, and their durations.

See “Event Logging” on page 2319.

For eventLogging-1.0 feature configuration information, see Event Logging.

### **ldapRegistry-3.0**

```
<feature>ldapRegistry-3.0</feature>
```

The ldapRegistry-3.0 feature provides support for LDAP user registry. The version 3.0 of the ldapRegistry-3.0 feature is compliant with the LDAP Version 3 specifications. The ldapRegistry-3.0 feature is not automatically enabled by the appSecurity-2.0 feature. Using this feature, you can federate multiple LDAP repositories. Two or more LDAP repositories can be configured in the server.xml file, and you can get the consolidated results from multiple repositories for all LDAP operations.

For ldapRegistry-3.0 feature configuration information, see “LDAP User Registry” on page 930.

### **Local JMX Connector**

```
<feature>localConnector-1.0</feature>
```

The localConnector-1.0 feature provides a local JMX connector that is built into the JVM. The JMX connector can be used only on the same host machine by someone running under the same user ID and the same JDK. It enables local access by JMX clients such as jConsole, or other JMX clients that use the Attach API.

See “Connecting to Liberty by using JMX” on page 1641.

For localConnector-1.0 feature configuration information, see “JMX Local Connector” on page 887.

#### 8.5.5.9 logstashCollector-1.0

```
<feature>logstashCollector-1.0</feature>
```

This feature gathers data from various sources and forwards the data to a Logstash server using Lumberjack protocol.

For logstashCollector-1.0 feature configuration information, see logstashCollector-1.0.

#### Monitoring

```
<feature>monitor-1.0</feature>
```

The monitor-1.0 feature provides Performance Monitoring Infrastructure (PMI) support on Liberty.

See Chapter 11, “Monitoring the Liberty server runtime environment,” on page 2267.

For monitor-1.0 feature configuration information, see “Performance Monitoring” on page 946.

#### OAuth

```
<feature>oauth-2.0</feature>
```

The oauth-2.0 feature provides support for securing access to resources using the OAuth 2.0 protocol.

For oauth-2.0 feature configuration information, see “OAuth” on page 936.

#### OpenID

```
<feature>openid-2.0</feature>
```

This feature enables users to authenticate themselves to multiple entities without the need to manage multiple accounts or sets of credentials. Liberty supports OpenID 2.0 and plays a role as a Relying Party in web single-sign-on. Accessing various entities like websites often requires a unique account that is associated with each entity. OpenID enables a single set of credentials that are handled by an OpenID Provider to grant access to any number of entities that support OpenID. See “OpenID” on page 1873.

For openid-2.0 feature configuration information, see “OpenID” on page 943.

#### OpenID Connect Client

```
<feature>openidConnectClient-1.0</feature>
```

This feature enables web applications to integrate OpenID Connect Client 1.0 for authenticating users instead of, or in addition to, the configured user registry. See “OpenID Connect” on page 1875.

For openidConnectClient-1.0 feature configuration information, see “OpenID Connect Client” on page 944.

#### OpenID Connect Provider

```
<feature>openidConnectServer-1.0</feature>
```

This feature enables web applications to integrate OpenID Connect Server 1.0 for authenticating users instead of, or in addition to, the configured user registry. See “OpenID Connect” on page 1875.

For openidConnectServer-1.0 feature configuration information, see “OpenID Connect Provider” on page 945.

#### OSGi Console

```
<feature>osgiConsole-1.0</feature>
```

This feature enables an OSGi console to aid the debugging of the runtime environment. It can be used to display information about bundles, packages, and services. This information can be useful when developing your own features for product extensions.

See “Using an OSGi console” on page 1587.

For `osgiConsole-1.0` feature configuration information, see “OSGi Debug Console” on page 941.

#### 8.5.5.9 Password Utilities

```
<feature>passwordUtilities-1.0</feature>
```

This feature enables support for obtaining AuthData from an application using security plug-points.

For `passwordUtilities-1.0` feature configuration information, see `passwordUtilities-1.0`.

#### 8.5.5.6 Request Timing

```
<feature>requestTiming-1.0</feature>
```

The `requestTiming-1.0` provides warnings and diagnostic information for the slow or hung requests.

See “Slow and hung request detection” on page 2321.

For `requestTiming-1.0` feature configuration information, see Request Timing.

### REST connector 1.0

```
<feature>restConnector-1.0</feature>
```

The `restConnector-1.0` feature provides a secure JMX connector that can be used locally or remotely using any JDK. It enables remote access by JMX clients through a REST-based connector and requires SSL and basic user security configuration.

See “Connecting to Liberty by using JMX” on page 1641 and, for details on REST connectors, see “Configuring secure JMX connection to Liberty” on page 1642.

**8.5.5.6** For information about using REST APIs to transfer files, see “Liberty: File transfer” on page 1660. For information about using REST APIs to transfer files to and from collective controllers, collective members, and registered hosts of a collective, see “Transferring files in a Liberty collective” on page 1660. To use the REST APIs, you add the `restConnector-1.0` feature to the server configuration.

For `restConnector-1.0` feature configuration information, see “JMX REST Connector 1.0” on page 887.

#### 8.5.5.7 SAML Web Browser SSO

```
<feature>samlWeb-2.0</feature>
```

The `samlWeb-2.0` feature enables web applications to delegate user authentication to a SAML identity provider instead of a configured user registry.

For `samlWeb-2.0` feature configuration information, see “SAML web single sign-on version 2.0” on page 948.

### Server status

```
<feature>serverStatus-1.0</feature>
```

The `serverStatus-1.0` feature enables Liberty servers to automatically publish their status to WebSphere Application Server deployment managers and job managers that are aware of the server as a resource in their Job configuration. The known states are Started and Stopped.

See Submitting jobs to manage Liberty servers and Installing Liberty server resources using the job manager.

For serverStatus-1.0 feature configuration information, see “Job Manager Integration” on page 929.

### **Session Persistence**

`<feature>sessionDatabase-1.0</feature>`

The sessionDatabase-1.0 feature provides session affinity and failover support on Liberty.

See “Configuring session persistence for Liberty” on page 1610.

For sessionDatabase-1.0 feature configuration information, see “Database Session Persistence” on page 870.

### **SPNEGO**

`<feature>spnego-1.0</feature>`

This feature enables users to log in to the Microsoft Domain controller once and access protected applications on Liberty servers without getting prompted again.

For more information on configuring SPNEGO on the Liberty server, see “Configuring SPNEGO authentication in Liberty” on page 1879.

For spnego-1.0 feature configuration information, see “Simple and Protected GSSAPI Negotiation Mechanism” on page 952.

### **Secure Sockets Layer (SSL)**

`<feature>ssl-1.0</feature>`

The ssl-1.0 feature provides support for Secure Sockets Layer (SSL) connections. To use the secure HTTPS listener, you must enable this feature. Liberty provides a dummy keystore and a dummy truststore, which are the same as those provided by previous versions of WebSphere Application Server. The secure HTTPS listener is not started unless the ssl-1.0 feature is enabled. If the feature is unavailable, the HTTPS listener is stopped. To specify the SSL certificates, add a pointer in the server.xml file; see “Securing communications in Liberty” on page 1833. To change the HTTPS port, set the `<httpsPort>` attribute of the `<httpEndpoint>` element in the server.xml file; see “Specifying Liberty bootstrap properties” on page 1437.

For ssl-1.0 feature configuration information, see “Secure Socket Layer” on page 951.

### **Timed Operations**

`<feature>timedOperations-1.0</feature>`

This feature enables support for warnings to be logged when certain operations in the application server are running more slowly than expected.

See “Liberty: Timed operations and JDBC calls” on page 2318.

For timedOperations-1.0 feature configuration information, see “Timed Operations” on page 955.

### **Dynamic caching service**

`<feature>webCache-1.0</feature>`

This feature enables local caching for web responses. It includes the Cache Service (distributedMap) feature and performs automatic caching of web application responses to improve response times and throughput. To customize the response caching, you can include a cache-spec.xml file in your applications. You can distribute the cache by adding a network cache provider such as WebSphere eXtreme Scale.

For webCache-1.0 feature configuration information, see “Web Response Cache” on page 957.

8.5.5.6

#### WebSphere MQ Messaging feature

`<feature>wmqJmsClient-2.0</feature>`

The `wmqJmsClient-2.0` feature provides applications with access to message queues hosted on IBM MQ through the JMS 2.0 API.

See “Deploying JMS applications to Liberty to use the IBM MQ messaging provider” on page 2197.

For `wmqJmsClient-2.0` feature configuration information, see “JMS 2.0 Client for IBM MQ” on page 883.

#### Web services security

`<feature>wsSecurity-1.1</feature>`

The `wsSecurity-1.1` feature provides support for securing web services at the message level. To secure web services messages, you must enable this feature and the `appSecurity-2.0` and `jaxws-2.2` features. Web services security policies defined in a WSDL file are ignored and are not enforced unless the `wsSecurity-1.1` feature is enabled.

See “Web services security” on page 2018.

For `wsSecurity-1.1` feature configuration information, see “Web Service Security” on page 957.

8.5.5.9

#### Web Services Atomic Transaction

`<feature>wsAtomicTransaction-1.2</feature>`

The `wsAtomicTransaction` is an interoperable transaction protocol. It enables you to flow distributed transactions by using Web service messages, and coordinate in an interoperable manner between heterogeneous transaction infrastructures.

For `wsAtomicTransaction-1.2` configuration information in Liberty, see “Web Services Atomic Transaction in Liberty” on page 2190.

### Systems Management

#### Administrative Center

`<feature>adminCenter-1.0</feature>`

The `adminCenter-1.0` feature is a web-based graphical interface for managing Liberty servers and applications and other resources from a web browser on a cell phone, tablet, or computer.

See “Administering Liberty using Admin Center” on page 1741 and “Admin Center feature restrictions” on page 2337.

For `adminCenter-1.0` feature configuration information, see “Admin Center” on page 855.

#### Cluster member

`<feature>clusterMember-1.0</feature>`

To add a member to a collective, add the `clusterMember-1.0` feature and optionally `<clusterMember name="cluster_name"/>` to its server configuration. The cluster name is published to the controller, and this server becomes part of the specified cluster.

See “Configuring a Liberty server cluster” on page 1155.

For `clusterMember-1.0` feature configuration information, see “Static Cluster Member” on page 953.

#### Collective controller

`<feature>collectiveController-1.0</feature>`

The `collectiveController-1.0` feature enables controller functionality for a management collective and includes a management repository MBean that is accessible using the

JMX/REST connector that is provided by the `restConnector-1.0` feature. The collective controller acts as a storage and collaboration mechanism to which collective members can connect. The `collectiveController-1.0` feature includes a `ServerCommandMbean` that can be used to remote start or stop servers that are managed by the collective controller. The `collectiveController-1.0` feature and its capabilities are available only in IBM WebSphere Application Server Liberty Network Deployment. The feature is not available in IBM WebSphere Application Server Liberty, IBM WebSphere Application Server Liberty - Express, or IBM WebSphere Application Server Liberty Core.

See “Setting up the server-management environment for Liberty by using collectives” on page 1134.

For `collectiveController-1.0` feature configuration information, see “Collective Controller” on page 864.

### Collective member

```
<feature>collectiveMember-1.0</feature>
```

The `collectiveMember-1.0` feature enables a server to be a member of a management collective, allowing it to be managed by the collective controller.

See “Setting up the server-management environment for Liberty by using collectives” on page 1134.

For `collectiveMember-1.0` feature configuration information, see “Collective Member” on page 866.

### Dynamic Routing

```
<feature>dynamicRouting-1.0</feature>
```

The Intelligent Management feature of the WebSphere plugin for Apache and IHS provides On Demand Router (ODR) capabilities for the plugin. This feature enables a server to run the dynamic routing service. The plugin can then connect to the ODR in order to dynamically route to all servers in the liberty collective.

See “Setting up dynamic routing for Liberty collectives” on page 1493.

For `dynamicRouting-1.0` feature configuration information, see “Dynamic Routing” on page 872.

8.5.5.7

### Health Analyzer

```
<feature>healthAnalyzer-1.0</feature>
```

The Health Analyzer feature provides health data collection for the health manager for the Intelligent Management feature Health Management. The health analyzer feature provides monitoring services to a member server. It registers as an analytics handler, collects the necessary stats (PMI, HealthCenter) via the analytics collector and analyses the conditions.

See “Configuring health management for Liberty” on page 1519.

For `healthAnalyzer-1.0` feature configuration information, see “Health Analyzer” on page 879.

8.5.5.7

### Health Manager

```
<feature>healthManager-1.0</feature>
```

The Health Manager feature provides health monitoring and automatic actions based on health policies for the Intelligent Management feature Health Management. The health

manager feature embodies the core functions of health management. Selecting this feature will also enable the default condition plugins. This feature requires the presence of the `collectiveController` feature.

See “Configuring health management for Liberty” on page 1519.

For `healthManager-1.0` feature configuration information, see “Health Manager” on page 880.

### Scaling Controller

```
<feature>scalingController-1.0</feature>
```

The `scalingController-1.0` feature makes scaling decisions for Liberty. Multiple servers can run the Scaling Controller feature for high availability purposes. Only one server is actively making scaling decisions at any time. If that server is stopped, another server that is running the Scaling Controller feature can take over making scaling decisions.

See “Setting up auto scaling for Liberty collectives” on page 1503.

For `scalingController-1.0` feature configuration information, see “Scaling Controller” on page 950.

### Scaling Member

```
<feature>scalingMember-1.0</feature>
```

The `scalingMember-1.0` feature can be added to the **featureManagement** element of the `server.xml` of servers that are collective members. This will enable auto clustering of the collective members and will allow the servers to dynamically start/stop based on criteria specified by the scaling policy. This feature works in conjunction with the scaling controller feature. The scaling controller feature should be enabled in the collective controllers that are part of the collective.

See “Setting up auto scaling for Liberty collectives” on page 1503.

For `scalingMember-1.0` feature configuration information, see “Scaling Member” on page 951.

## z/OS

### z/OS Connect

```
<feature>zosConnect-1.0</feature>
```

The `zosConnect-1.0` feature is service that encapsulates calling z/OS target applications using REST calls.

**z/OS** See “Setting up z/OS Connect” on page 1536.

**z/OS** For `zosConnect-1.0` feature configuration information, see “z/OS Connect” on page 959.

#### 8.5.5.7 z/OS Connect 1.2

```
<feature>zosConnect-1.2</feature>
```

This feature provides a gateway between mobile, cloud, and web clients and z/OS back-end systems, such as CICS Transaction Server, IMS, and batch applications. It provides RESTful APIs and enables you to route HTTP requests to remote REST endpoints. It also accepts and returns JSON payloads and communicates with back-end systems by providing a data transformation service that converts JSON payloads to/from byte arrays consumable by z/OS native-language applications written in Cobol, PL/I, and C.

For more information, see “IBM z/OS Connect overview” on page 1020

**z/OS** For `zosConnect-1.2` feature configuration information, see “z/OS Connect 1.2” on page 960.

### **z/OS optimized local adapters**

`<feature>zosLocalAdapters-1.0</feature>`

The `zosLocalAdapters-1.0` feature enables high-performance calling between native-language applications on z/OS and business logic in a Liberty server environment.

**z/OS** See “Optimized local adapters on Liberty for z/OS” on page 1690 and “Enabling the Liberty server environment to use optimized local adapters” on page 1697.

**z/OS** For `zosLocalAdapters-1.0` feature configuration information, see “z/OS Optimized Local Adapters” on page 961.

### **z/OS security**

`<feature>zosSecurity-1.0</feature>`

The `zosSecurity-1.0` feature provides support on the z/OS platform for basic interactions with the SAF Registry, including authenticating users, and retrieving users, groups, or groups associated with users, from the SAF Registry.

**z/OS** See “Activating and configuring the SAF registry on z/OS” on page 1857.

**z/OS** For `zosSecurity-1.0` feature configuration information, see “z/OS SAF Integration” on page 962.

### **z/OS transaction management**

`<feature>zosTransaction-1.0</feature>`

Specifying this feature enables the application server to synchronize and appropriately manage transactional activity between the Resource Recovery Services (RRS), the transaction manager of the application server, and the resource manager.

**z/OS** See “Enabling a DB2 JDBC Type 2 driver on z/OS” on page 1681 and “Liberty:Runtime environment known issues and restrictions” on page 2333.

**z/OS** For `zosTransaction-1.0` feature configuration information, see “z/OS Transaction Management” on page 963.

### **z/OS workload management**

`<feature>zosWlm-1.0</feature>`

The `zosWlm-1.0` feature provides access to z/OS native workload management (WLM) services.

**z/OS** See “Enabling workload management for Liberty on z/OS” on page 1736.

**z/OS** For `zosWlm-1.0` feature configuration information, see “z/OS Workload Management” on page 963.

## **Java EE 6 Web Profile**

### **Bean validation**

`<feature>beanValidation-1.0</feature>`

The `beanValidation-1.0` feature provides validations for JavaBeans at each layer of an application. The validation can be applied to all layers of JavaBeans in an application by using annotations or a `validation.xml` deployment descriptor.

See “Bean validation feature restrictions” on page 2337.

For `beanValidation-1.0` feature configuration information, see “Bean Validation 1.0” on page 862.

**CDI** `<feature>cdi-1.0</feature>`

The `cdi-1.0` feature enables support for the Contexts and Dependency Injection 1.0 specification on Liberty.

See “Administering Contexts and Dependency Injection applications on Liberty” on page 1725.

For `cdi-1.0` feature configuration information, see “Contexts and Dependency Injection 1.0” on page 867.

### **Enterprise JavaBeans (EJB) Lite subset**

```
<feature>ejbLite-3.1</feature>
```

The `ejbLite-3.1` feature provides support for EJB applications written to the EJB Lite subset of the EJB 3.1 specification.

The following functions are supported:

- An EJB module packaged in an EAR file.
- EJBs packaged in a WAR file.
- The `@Stateful`, `@Stateless`, `@Singleton`, and `@EJB` annotations.
- The `javax.annotation.security` annotations.
- Injection of JPA `EntityManager`, `EntityManagerFactory`, and JDBC `DataSource` into all types of session bean types.
- `ejb-jar.xml`.
- EJB interceptors.
- No-Interface View.
- Bean managed transactions (`UserTransaction`).

See “`ejbLite-3.1` feature restrictions” on page 2338.

For `ejbLite-3.1` feature configuration information, see “Enterprise JavaBeans Lite 3.1” on page 874.

### **Java Database Connectivity (JDBC)**

```
<feature>jdbc-4.0</feature>
```

You can take an existing application that uses Java Database Connectivity (JDBC) and a data source, and deploy the application to a server. The `jdbc-4.0` feature provides support for applications that access a database.

See “Deploying an existing JDBC application to Liberty” on page 2150.

For `jdbc-4.0` feature configuration information, see “Java Database Connectivity 4.0” on page 894.

### **Java Naming and Directory Interface (JNDI)**

```
<feature>jndi-1.0</feature>
```

The `jndi-1.0` feature provides support for a single JNDI entry definition in the server configuration of Liberty.

For `jndi-1.0` feature configuration information, see “Java Naming and Directory Interface” on page 902.

### **Java Persistence API (JPA)**

```
<feature>jpa-2.0</feature>
```

The `jpa-2.0` feature provides support for applications that use application-managed and container-managed JPA written to the JPA 2.0 specification. The support is built on Apache OpenJPA with extensions to support the container-managed programming model.

Extended Persistence Context is now available for use with Stateful Session beans.

See “Deploying a JPA application to Liberty” on page 2157.

For jpa-2.0 feature configuration information, see “Java Persistence API 2.0” on page 903.

### **JavaServer Faces (JSF)**

```
<feature>jsf-2.0</feature>
```

The jsf-2.0 feature provides support for web applications that use the JSF framework. This framework simplifies the construction of user interfaces. If you include the jsf-2.0 feature, you also include the jsp-2.2 feature, because the JSF framework is an extension of the JSP framework.

For jsf-2.0 feature configuration information, see “JavaServer Faces 2.0” on page 925.

### **JavaServer Pages (JSP)**

```
<feature>jsp-2.2</feature>
```

If you include the jsf-2.0 feature, you also include the jsp-2.2 feature, because the JSF framework is an extension of the JSP framework. If you include the jsp-2.2 feature, you also include the servlet-3.0 feature.

See “jsp-2.2 feature restrictions” on page 2339.

For jsp-2.2 feature configuration information, see “JavaServer Pages 2.2” on page 927.

### **Servlet 3.0**

```
<feature>servlet-3.0</feature>
```

The servlet-3.0 feature provides support for HTTP Servlets written to the Java Servlet 3.0 specification.

See Chapter 8, “Securing Liberty and its applications,” on page 1829.

For servlet-3.0 feature configuration information, see “Java Servlets 3.0” on page 915.

### **Web Profile**

```
<feature>webProfile-6.0</feature>
```

This feature provides a convenient combination of the Liberty features that are required to support the Java EE 6.0 Web Profile.

For webProfile-6.0 feature configuration information, see “Java EE Web Profile 6.0” on page 899.

## **Java EE 6 Technologies**

### **Java Architecture for XML Binding (JAXB)**

```
<feature>jaxb-2.2</feature>
```

The jaxb-2.2 feature provides support for the Java Architecture for XML Binding (JAXB) on Liberty.

See JAXB and “jaxb-2.2 feature restriction” on page 2338.

For jaxb-2.2 feature configuration information, see “Java XML Bindings 2.2” on page 922.

### **Java API for RESTful Web Services (JAX-RS)**

```
<feature>jaxrs-1.1</feature>
```

The jaxrs-1.1 feature provides support for the Java API for RESTful Web Services on Liberty.

- For EJB applications that use the jaxrs-1.1 server feature, you must enable the ejbLite-3.1 feature in the server.xml file.
- For JAX-RS applications that use CDI, you must enable the cdi-1.0 feature in the server.xml file.
- For applications that use the global handler services, you must enable the jaxrs-1.1 or the jaxws-2.2 feature in the server.xml file.

For jaxrs-1.1 feature configuration information, see “Java RESTful Services 1.1” on page 911.

### **Java API for XML-Based Web Services (JAX-WS)**

```
<feature>jaxws-2.2</feature>
```

The jaxws-2.2 feature provides support for the Java API for XML-Based Web Services on Liberty.

- For web applications that support the JAX-WS programming model, you must enable the servlet-3.0 and jaxws-2.2 server features in the server.xml file.
- For EJB applications that support the JAX-WS programming model, you must enable the ejbLite-3.1, servlet-3.0, and jaxws-2.2 server features in the server.xml file.
- For applications that use the global handler services, you must enable the jaxrs-1.1 or the jaxws-2.2 feature in the server.xml file.

See “jaxws-2.2 feature restrictions” on page 2339.

For jaxws-2.2 feature configuration information, see “Java Web Services 2.2” on page 920.

### **Java EE Connector Architecture**

```
<feature>jca-1.6</feature>
```

The jca-1.6 feature provides configuration elements to define instances of connection factories, administered objects, and activation specifications, and to associate these instances with an installed resource adapter.

For jca-1.6 feature configuration information, see “Java Connector Architecture 1.6” on page 892.

### **Java EE Connector Architecture Inbound Security**

```
<feature>jcaInboundSecurity-1.0</feature>
```

The jcaInboundSecurity-1.0 feature enables security inflow for resource adapters.

For jcaInboundSecurity-1.0 feature configuration information, see “Java Connector Architecture 1.0 Security Inflow” on page 891.

### **Java Message Service 1.1**

```
<feature>jms-1.1</feature>
```

The jms-1.1 feature enables the configuration of resource adapters to access messaging systems using the Java Message Service API. This also includes the configuration JMS connection factories, queues, topics, and activation specifications. Any JMS resource adapter that complies with the JCA 1.6 specification can be used.

For jms-1.1 feature configuration information, see “Java Message Service 1.1” on page 900.

### **Message-Driven beans**

```
<feature>jmsMdb-3.1</feature>
```

The jmsMdb-3.1 feature provides support for deploying and configuring the JMS resources that are required for the message-driven beans (MDB) to run within Liberty. This feature enables MDB to interact with either the embedded Liberty messaging or WebSphere MQ.

For jmsMdb-3.1 feature configuration information, see “JMS Message-Driven Beans 3.1” on page 885.

### **Message-Driven Beans 3.1**

```
<feature>mdb-3.1</feature>
```

The mdb-3.1 feature enables the use of Message-Driven Enterprise JavaBeans. MDBs allow asynchronous processing of messages within a Java EE component.

For mdb-3.1 feature configuration information, see “Message-Driven Beans 3.1” on page 934.

### **Embedded Liberty Messaging features**

`<feature>wasJmsClient-1.1</feature>`

The `wasJmsClient-1.1` feature enables support for JMS resource configurations (such as the connection factories, activation specifications, and queue and topic resources) and also provides the client libraries that are required by the messaging applications to connect to the JMS server on Liberty.

See “Enabling JMS messaging for Liberty” on page 1121 and “Deploying messaging applications to Liberty” on page 2195.

For `wasJmsClient-1.1` feature configuration information, see “JMS 1.1 Client for Message Server” on page 882.

`<feature>wasJmsSecurity-1.0</feature>`

The `wasJmsSecurity-1.0` feature supports secure connections to the messaging engine. When the `wasJmsSecurity-1.0` feature is enabled, it starts authenticating and authorizing the users who are trying to connect to the messaging engine. The user is authenticated against the registry that is defined in the `server.xml` file. When the user wants to access a destination such as a topic or a queue, then the user must be granted the required permissions. The access to the destination is defined in the `<messagingSecurity>` element (the child element of the `messagingEngine` element) in the `server.xml` file. If the `wasJmsSecurity-1.0` feature is added and the `<messagingSecurity>` element is not defined in the `server.xml` file, then the users cannot connect to the messaging engine or perform any messaging action (for example, sending or receiving messages from the destinations). For `wasJmsSecurity-1.0` feature configuration information, see “Message Server Security 1.0” on page 933.

#### **Notes:**

- Configuring the user registry is a prerequisite for the `wasJmsSecurity-1.0` feature. Ensure that a user registry is configured before the `wasJmsSecurity-1.0` feature is enabled.
- When you enable the `wasJmsSecurity-1.0` feature, you must also configure the `<messagingSecurity>` element, which is the child element of the `<messagingEngine>` element, in the `server.xml` file. This configuration enables authorized users to access messaging destinations.

`<feature>wasJmsServer-1.0</feature>`

The `wasJmsServer-1.0` feature enables the JMS messaging engine run time to be initialized. The messaging run time is responsible for providing the application connectivity, managing the state of destinations such as topics or queues, and handling quality of service, security, and transactions. This feature also provides support for the inbound connections from the remote messaging applications. The remote messaging applications can connect to the JMS messaging engine through TCP/IP over SSL or non-SSL.

To connect using SSL, you must enable the SSL feature.

See “Enabling secure JMS messaging for Liberty” on page 1126.

For `wasJmsServer-1.0` feature configuration information, see “Message Server 1.0” on page 932.

### **WebSphere MQ Messaging feature**

`<feature>wmqJmsClient-1.1</feature>`

The `wmqJmsClient-1.1` feature enables applications to use JMS messaging that connects to a IBM MQ server.

See “Deploying JMS applications to Liberty to use the IBM MQ messaging provider” on page 2197.

For `wmqJmsClient-1.1` feature configuration information, see “JMS 1.1 Client for IBM MQ” on page 881.

## API Discovery 1.0

Enables discovery and exposure of REST APIs within Liberty.

### Enabling this feature

To enable the API Discovery 1.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>apiDiscovery-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the API Discovery 1.0 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.apiDiscovery-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `distributedMap-1.0` - Distributed Map interface for Dynamic Caching
- `json-1.0` - JavaScript Object Notation for Java
- `servlet-3.0` - Java Servlets 3.0
- `servlet-3.1` - Java Servlets 3.1
- `ssl-1.0` - Secure Socket Layer

### Third party API packages provided by this feature

- `io.swagger.annotations`

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the API Discovery 1.0 feature:

- `administrator-role`
- `apiDiscovery`
- `authCache`
- `authentication`
- `authorization-roles`
- `basicRegistry`
- `channelfw`
- `classloading`
- `httpAccessLogging`
- `httpDispatcher`
- `httpEncoding`
- `httpEndpoint`
- `httpOptions`
- `httpProxyRedirect`

- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- mimeTypees
- quickStartSecurity
- tcpOptions
- trustAssociation
- virtualHost

## Admin Center

The adminCenter-1.0 feature enables the Liberty Admin Center, a web-based graphical interface for deploying, monitoring and managing Liberty servers in standalone and collective environments.

### Enabling this feature

To enable the Admin Center feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>adminCenter-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Admin Center feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.adminCenter-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- distributedMap-1.0 - Distributed Map interface for Dynamic Caching
- json-1.0 - JavaScript Object Notation for Java
- jsp-2.2 - JavaServer Pages 2.2
- jsp-2.3 - JavaServer Pages 2.3
- restConnector-1.0 - JMX REST Connector 1.0
- restConnector-2.0 - JMX REST Connector 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1
- ssl-1.0 - Secure Socket Layer

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Admin Center feature:

- administrator-role
- authCache
- authentication
- authorization-roles
- basicRegistry
- channelfw
- classloading
- httpAccessLogging
- httpDispatcher

- httpEncoding
- httpEndpoint
- httpOptions
- httpProxyRedirect
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- mimeTypes
- quickStartSecurity
- tcpOptions
- trustAssociation
- virtualHost

## Application Client Support for Server

This feature enables the Liberty server to process client modules and support remote client containers.

### Enabling this feature

To enable the Application Client Support for Server feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>appClientSupport-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Application Client Support for Server feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.appClientSupport-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- jndi-1.0 - Java Naming and Directory Interface

### Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Application Client Support for Server feature:

- application
- applicationManager
- applicationMonitor
- channelfw
- classloading
- enterpriseApplication
- iiopEndpoint
- iiopServerPolicies
- javaPermission
- library

- orb
- tcpOptions
- webApplication

## Application Security 1.0

This feature is superseded by appSecurity-2.0. Support for securing the server runtime environment and applications. This feature enables servlet-3.0 and web application security, support for LDAP and basic user registries, and SSL. To support secure EJB applications, you must add the ejbLite-3.1 feature. When you add this feature to your server, you need to configure a user registry, such as the basic user registry or the LDAP user registry.

### Enabling this feature

To enable the Application Security 1.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>appSecurity-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Application Security 1.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.appSecurity-1.0; type="osgi.subsystem.feature"
```

### Features that this feature is superseded by

- ldapRegistry-3.0 - LDAP User Registry
- servlet-3.0 - Java Servlets 3.0
- appSecurity-2.0 - Application Security 2.0

### Features that this feature enables

- appSecurity-2.0 - Application Security 2.0
- ldapRegistry-3.0 - LDAP User Registry
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### Features that enable this feature

- passwordUtilities-1.0 - Password Utilities

## Application Security 2.0

This feature enables support for securing the server runtime environment and applications; it includes a basic user registry. This feature supersedes appSecurity-1.0 and does not include servlet-3.0 or support for the LDAP user registry. To secure web applications, add the servlet-3.0 feature. To secure EJB applications, add the ejbLite-3.1 feature. To use LDAP, add the ldapRegistry-3.0 feature. When you add the appSecurity-2.0 feature to your server, you need to configure a user registry, such as the basic user registry or the LDAP user registry.

### Enabling this feature

To enable the Application Security 2.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>appSecurity-2.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Application Security 2.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:  
`com.ibm.websphere.appserver.appSecurity-2.0; type="osgi.subsystem.feature"`

## Features that this feature enables

- ssl-1.0 - Secure Socket Layer

## Features that enable this feature

- appSecurity-1.0 - Application Security 1.0
- constrainedDelegation-1.0 - Kerberos Constrained Delegation for SPNEGO
- jacc-1.5 - Java Authorization Contract for Containers 1.5
- jaspic-1.1 - Java Authentication SPI for Containers 1.1
- oauth-2.0 - OAuth
- openid-2.0 - OpenID
- passwordUtilities-1.0 - Password Utilities
- samlWeb-2.0 - SAML web single sign-on version 2.0
- spnego-1.0 - Simple and Protected GSSAPI Negotiation Mechanism
- webProfile-6.0 - Java EE Web Profile 6.0
- webProfile-7.0 - Java EE Web Profile 7.0
- wsSecurity-1.1 - Web Service Security

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Application Security 2.0 feature:

- administrator-role
- authCache
- authentication
- basicRegistry
- classloading
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- quickStartSecurity

## Application Security for Client 1.0

Support for securing the client container runtime environment and applications. This feature enables application security, CSIV2 and SSL on the client.

## Enabling this feature

To enable the Application Security for Client 1.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>appSecurityClient-1.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Application Security for Client 1.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.appSecurityClient-1.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- ssl-1.0 - Secure Socket Layer

## IBM API packages provided by this feature

- com.ibm.websphere.security
- com.ibm.websphere.security.auth.callback
- com.ibm.wsspi.security.auth.callback

## Feature configuration elements

You can use the following elements in your server.xml file to configure the Application Security for Client 1.0 feature:

- channelfw
- jaasLoginContextEntry
- jaasLoginModule
- orb
- tcpOptions

## Basic Extensions using Liberty Libraries

This feature enables the configuration of Basic Extensions using Liberty Libraries (BELL).

## Enabling this feature

To enable the Basic Extensions using Liberty Libraries feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>bells-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Basic Extensions using Liberty Libraries feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.bells-1.0; type="osgi.subsystem.feature"
```

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Basic Extensions using Liberty Libraries feature:

- `bell`
- `classloading`
- `library`

## Batch API 1.0

This feature enables support for the Java Batch 1.0 API specified by JSR-352.

### Enabling this feature

To enable the Batch API 1.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>batch-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Batch API 1.0 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.batch-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `jdbc-4.0` - Java Database Connectivity 4.0
- `jdbc-4.1` - Java Database Connectivity 4.1
- `jndi-1.0` - Java Naming and Directory Interface
- `servlet-3.1` - Java Servlets 3.1

### Features that enable this feature

- `batchManagement-1.0` - Batch Management
- `javaee-7.0` - Java EE Full Platform 7.0

### Standard API packages provided by this feature

- `javax.batch.api`
- `javax.batch.api.chunk`
- `javax.batch.api.chunk.listener`
- `javax.batch.api.listener`
- `javax.batch.api.partition`
- `javax.batch.operations`
- `javax.batch.runtime`
- `javax.batch.runtime.context`
- `javax.inject`

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Batch API 1.0 feature:

- `batchPersistence`
- `classloading`
- `databaseStore`

- transaction

## Batch Management

This feature provides managed batch support for the Java batch container. This includes the Batch REST management interface, job logging support, and a command line utility for external scheduler integration.

### Enabling this feature

To enable the Batch Management feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>batchManagement-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Batch Management feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.batchManagement-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- batch-1.0 - Batch API 1.0
- distributedMap-1.0 - Distributed Map interface for Dynamic Caching
- jdbc-4.0 - Java Database Connectivity 4.0
- jdbc-4.1 - Java Database Connectivity 4.1
- json-1.0 - JavaScript Object Notation for Java
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1
- ssl-1.0 - Secure Socket Layer

### Standard API packages provided by this feature

- javax.batch.api
- javax.batch.api.chunk
- javax.batch.api.chunk.listener
- javax.batch.api.listener
- javax.batch.api.partition
- javax.batch.operations
- javax.batch.runtime
- javax.batch.runtime.context

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Batch Management feature:

- administrator-role
- authCache
- authentication
- authorization-roles
- basicRegistry
- batchJobLogging
- channelfw
- classloading

- httpAccessLogging
- httpDispatcher
- httpEncoding
- httpEndpoint
- httpOptions
- httpProxyRedirect
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- mimeTypees
- quickStartSecurity
- tcpOptions
- transaction
- trustAssociation
- virtualHost

## Bean Validation 1.0

The Bean Validation 1.0 specification provides an annotation based model for validating JavaBeans. It can be used to assert and maintain the integrity of data as it travels through an application.

### Enabling this feature

To enable the Bean Validation 1.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>beanValidation-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Bean Validation 1.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.beanValidation-1.0; type="osgi.subsystem.feature"
```

### Features that enable this feature

- jpa-2.0 - Java Persistence API 2.0
- jsf-2.0 - JavaServer Faces 2.0
- osgi.jpa-1.0 - OSGi Java Persistence API
- webProfile-6.0 - Java EE Web Profile 6.0

### Standard API packages provided by this feature

- javax.validation
- javax.validation.bootstrap
- javax.validation.constraints
- javax.validation.groups
- javax.validation.metadata
- javax.validation.spi

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Bean Validation 1.0 feature:

- `classloading`
- `library`

## Bean Validation 1.1

The Bean Validation 1.1 specification provides an annotation based model for validating JavaBeans. It can be used to assert and maintain the integrity of data as it travels through an application.

## Enabling this feature

To enable the Bean Validation 1.1 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>beanValidation-1.1</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Bean Validation 1.1 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.beanValidation-1.1; type="osgi.subsystem.feature"
```

## Features that this feature enables

- `el-3.0` - Expression Language 3.0

## Features that enable this feature

- `javaeeClient-7.0` - Java EE V7 Application Client
- `jpa-2.0` - Java Persistence API 2.0
- `jsf-2.0` - JavaServer Faces 2.0
- `osgi.jpa-1.0` - OSGi Java Persistence API
- `webProfile-7.0` - Java EE Web Profile 7.0

## Standard API packages provided by this feature

- `javax.validation`
- `javax.validation.bootstrap`
- `javax.validation.constraints`
- `javax.validation.constraintvalidation`
- `javax.validation.executable`
- `javax.validation.groups`
- `javax.validation.metadata`
- `javax.validation.spi`

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Bean Validation 1.1 feature:

- `classloading`
- `library`
- `transaction`

## Cloudant Integration 1.0

This feature enables connections to Cloudant by providing a connector instance configured in the server configuration, which can be injected or accessed through JNDI. Applications use the Cloudant client library to utilize the connector instance.

### Enabling this feature

To enable the Cloudant Integration 1.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>cloudant-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Cloudant Integration 1.0 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.cloudant-1.0; type="osgi.subsystem.feature"
```

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Cloudant Integration 1.0 feature:

- `authData`
- `classloading`
- `cloudant`
- `cloudantDatabase`
- `library`

## Collective Controller

The collective controller feature allows a server to become the controller for a management collective. The collective controller acts as a command and control mechanism for administrative functions for the collective, and serves as a storage and collaboration mechanism for the collective and cluster members.

### Enabling this feature

To enable the Collective Controller feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>collectiveController-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Collective Controller feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.collectiveController-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `collectiveMember-1.0` - Collective Member
- `distributedMap-1.0` - Distributed Map interface for Dynamic Caching
- `json-1.0` - JavaScript Object Notation for Java
- `restConnector-1.0` - JMX REST Connector 1.0

- restConnector-2.0 - JMX REST Connector 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1
- ssl-1.0 - Secure Socket Layer

### **Features that enable this feature**

- dynamicRouting-1.0 - Dynamic Routing
- healthManager-1.0 - Health Manager
- scalingController-1.0 - Scaling Controller

### **IBM API packages provided by this feature**

- com.ibm.websphere.collective.controller
- com.ibm.websphere.collective.repository

### **Feature configuration elements**

You can use the following elements in your `server.xml` file to configure the Collective Controller feature:

- administrator-role
- authCache
- authentication
- authorization-roles
- basicRegistry
- channelfw
- classloading
- clusterPluginConfig
- collectiveController
- collectiveRepository
- deployManager
- deployRule
- deployVariable
- hostAccess
- httpAccessLogging
- httpDispatcher
- httpEncoding
- httpEndpoint
- httpOptions
- httpProxyRedirect
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- mimeTypeypes
- quickStartSecurity
- serverCommands
- tcpOptions
- trustAssociation

- virtualHost

## Collective Member

This feature enables a server to be a member of a management collective.

### Enabling this feature

To enable the Collective Member feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>collectiveMember-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Collective Member feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.collectiveMember-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- restConnector-1.0 - JMX REST Connector 1.0
- restConnector-2.0 - JMX REST Connector 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### Features that enable this feature

- clusterMember-1.0 - Static Cluster Member
- collectiveController-1.0 - Collective Controller
- healthAnalyzer-1.0 - Health Analyzer
- scalingMember-1.0 - Scaling Member

### SPI packages provided by this feature

- com.ibm.wsspi.collective.repository
- com.ibm.wsspi.collective.repository.publisher

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Collective Member feature:

- collectiveCertificate
- collectiveMember
- hostAuthInfo
- hostSingleton

## Concurrency Utilities for Java EE 1.0

This feature enables the creation of managed executors that allow applications to submit tasks to run concurrently, with thread context that is managed by the application server. It also enables the creation of managed thread factories to create threads that run with the thread context of the component that looks up the managed thread factory.

### Enabling this feature

To enable the Concurrency Utilities for Java EE 1.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>concurrent-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Concurrency Utilities for Java EE 1.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.concurrent-1.0; type="osgi.subsystem.feature"
```

## Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0

## Standard API packages provided by this feature

- javax.enterprise.concurrent

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Concurrency Utilities for Java EE 1.0 feature:

- `classloading`
- `contextService`
- `managedExecutorService`
- `managedScheduledExecutorService`
- `managedThreadFactory`

## Contexts and Dependency Injection 1.0

The Contexts and Dependency Injection specification makes it easier to integrate Java EE components of different types. It provides a common mechanism to inject component such as EJBs or Managed Beans into other components such as JSPs or other EJBs.

## Enabling this feature

To enable the Contexts and Dependency Injection 1.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>cdi-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Contexts and Dependency Injection 1.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.cdi-1.0; type="osgi.subsystem.feature"
```

## Features that enable this feature

- webProfile-6.0 - Java EE Web Profile 6.0

## Standard API packages provided by this feature

- javax.decorator
- javax.enterprise.context
- javax.enterprise.context.spi
- javax.enterprise.event
- javax.enterprise.inject
- javax.enterprise.inject.spi
- javax.enterprise.util
- javax.inject
- javax.interceptor

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Contexts and Dependency Injection 1.0 feature:

- `cdiContainer`
- `classloading`
- `transaction`

## Contexts and Dependency Injection 1.2

The Contexts and Dependency Injection specification makes it easier to integrate Java EE components of different types. It provides a common mechanism to inject component such as EJBs or Managed Beans into other components such as JSPs or other EJBs.

## Enabling this feature

To enable the Contexts and Dependency Injection 1.2 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>cdi-1.2</feature>
```

## Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Contexts and Dependency Injection 1.2 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.cdi-1.2; type="osgi.subsystem.feature"
```

## Features that enable this feature

- `javaeeClient-7.0` - Java EE V7 Application Client
- `microProfile-1.0` - Micro Profile 1.0
- `webProfile-7.0` - Java EE Web Profile 7.0

## Standard API packages provided by this feature

- javax.decorator
- javax.enterprise.context
- javax.enterprise.context.spi

- javax.enterprise.event
- javax.enterprise.inject
- javax.enterprise.inject.spi
- javax.enterprise.util
- javax.inject
- javax.interceptor

### Third party API packages provided by this feature

- org.jboss.weld.context
- org.jboss.weld.context.api
- org.jboss.weld.context.beanstore
- org.jboss.weld.context.bound
- org.jboss.weld.context.conversation

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Contexts and Dependency Injection 1.2 feature:

- application
- applicationManager
- applicationMonitor
- cdi12
- classloading
- javaPermission
- library
- transaction

### CouchDB Integration 1.0

This feature enables connections to CouchDB by providing a connector instance configured in the server configuration, which can be injected or accessed through JNDI. Applications use the ektor client library to utilize the connector instance to work with CouchDB.

### Enabling this feature

To enable the CouchDB Integration 1.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>couchdb-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the CouchDB Integration 1.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.couchdb-1.0; type="osgi.subsystem.feature"
```

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the CouchDB Integration 1.0 feature:

- `classloading`
- `couchdb`
- `library`

## Database Session Persistence

This feature enables persistence of HTTP sessions to a datasource using JDBC. Persisting HTTP session data to a database allows recovery of the data after a server restart or unexpected server failure. Failover of HTTP sessions can be achieved by configuring multiple servers to persist data to the same location

### Enabling this feature

To enable the Database Session Persistence feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>sessionDatabase-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Database Session Persistence feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.sessionDatabase-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `jdbc-4.0` - Java Database Connectivity 4.0
- `jdbc-4.1` - Java Database Connectivity 4.1
- `jndi-1.0` - Java Naming and Directory Interface

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Database Session Persistence feature:

- `classloading`
- `httpSession`
- `httpSessionDatabase`
- `transaction`

## Distributed Map interface for Dynamic Caching

This feature provides a local cache service which can be accessed through the `DistributedMap` API. A default cache is bound in JNDI at `"services/cache/distributedmap"`. Caches can be distributed through addition of a network cache provider such as WebSphere eXtreme Scale.

### Enabling this feature

To enable the Distributed Map interface for Dynamic Caching feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>distributedMap-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Distributed Map interface for Dynamic Caching feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.distributedMap-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- jndi-1.0 - Java Naming and Directory Interface

### Features that enable this feature

- adminCenter-1.0 - Admin Center
- apiDiscovery-1.0 - API Discovery 1.0
- batchManagement-1.0 - Batch Management
- collectiveController-1.0 - Collective Controller
- dynamicRouting-1.0 - Dynamic Routing
- oauth-2.0 - OAuth
- openidConnectClient-1.0 - OpenID Connect Client
- restConnector-1.0 - JMX REST Connector 1.0
- restConnector-2.0 - JMX REST Connector 2.0
- samlWeb-2.0 - SAML web single sign-on version 2.0
- scim-1.0 - System for Cross-domain Identity Management
- webCache-1.0 - Web Response Cache
- wsAtomicTransaction-1.2 - WS-AT Service
-  zosConnect-1.0 - z/OS Connect
-  zosConnect-1.2 - z/OS Connect 1.2

### IBM API packages provided by this feature

- com.ibm.websphere.cache
- com.ibm.websphere.cache.exception
- com.ibm.websphere.exception
- com.ibm.ws.cache.spi
- com.ibm.wsspi.cache

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Distributed Map interface for Dynamic Caching feature:

- classloading
- distributedMap
- library

## Dynamic Routing

The Intelligent Management feature of the WebSphere plug-in for Apache and IHS provides On Demand Router capabilities for the plug-in. This feature enables a server to run a REST service to which the plug-in can connect in order to dynamically route to all servers in the liberty collective.

### Enabling this feature

To enable the Dynamic Routing feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>dynamicRouting-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Dynamic Routing feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.dynamicRouting-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- collectiveController-1.0 - Collective Controller
- distributedMap-1.0 - Distributed Map interface for Dynamic Caching
- json-1.0 - JavaScript Object Notation for Java
- restConnector-1.0 - JMX REST Connector 1.0
- restConnector-2.0 - JMX REST Connector 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1
- ssl-1.0 - Secure Socket Layer

### IBM API packages provided by this feature

- com.ibm.websphere.dynamic.routing

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Dynamic Routing feature:

- administrator-role
- authCache
- authentication
- authorization-roles
- basicRegistry
- channelfw
- classloading
- dynamicRouting
- httpAccessLogging
- httpDispatcher
- httpEncoding
- httpEndpoint
- httpOptions
- httpProxyRedirect
- jaasLoginContextEntry
- jaasLoginModule

- library
- ltpa
- mimeTypees
- quickStartSecurity
- tcpOptions
- trustAssociation
- virtualHost

## Enterprise JavaBeans 3.2

This feature enables support for Enterprise JavaBeans written to the EJB 3.2 specification.

### Enabling this feature

To enable the Enterprise JavaBeans 3.2 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>ejb-3.2</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Enterprise JavaBeans 3.2 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.ejb-3.2; type="osgi.subsystem.feature"
```

### Features that this feature enables

- ejbHome-3.2 - Enterprise JavaBeans Home Interfaces 3.2
- ejbLite-3.2 - Enterprise JavaBeans Lite 3.2
- ejbPersistentTimer-3.2 - Enterprise JavaBeans Persistent Timers 3.2
- ejbRemote-3.2 - Enterprise JavaBeans Remote 3.2
- mdb-3.2 - Message-Driven Beans 3.2

### Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Enterprise JavaBeans 3.2 feature:

- classloading
- transaction

## Enterprise JavaBeans Home Interfaces 3.2

This feature enables the use of home interfaces in Enterprise JavaBeans.

### Enabling this feature

To enable the Enterprise JavaBeans Home Interfaces 3.2 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>ejbHome-3.2</feature>
```

### Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Enterprise JavaBeans Home Interfaces 3.2 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.ejbHome-3.2; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `ejbLite-3.2` - Enterprise JavaBeans Lite 3.2

### Features that enable this feature

- `ejb-3.2` - Enterprise JavaBeans 3.2

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Enterprise JavaBeans Home Interfaces 3.2 feature:

- `classloading`
- `transaction`

## Enterprise JavaBeans Lite 3.1

This feature enables support for Enterprise JavaBeans written to the EJB Lite subset of the EJB 3.1 specification.

### Enabling this feature

To enable the Enterprise JavaBeans Lite 3.1 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>ejbLite-3.1</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Enterprise JavaBeans Lite 3.1 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.ejbLite-3.1; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `jndi-1.0` - Java Naming and Directory Interface

### Features that enable this feature

- `webProfile-6.0` - Java EE Web Profile 6.0
- `z/OS` `zosLocalAdapters-1.0` - z/OS Optimized Local Adapters

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Enterprise JavaBeans Lite 3.1 feature:

- `application`

- applicationManager
- applicationMonitor
- classloading
- ejbApplication
- ejbContainer
- enterpriseApplication
- javaPermission
- library
- transaction
- webApplication

## Enterprise JavaBeans Lite 3.2

This feature enables support for Enterprise JavaBeans written to the EJB Lite subset of the EJB 3.2 specification.

### Enabling this feature

To enable the Enterprise JavaBeans Lite 3.2 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>ejbLite-3.2</feature>
```

### Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Enterprise JavaBeans Lite 3.2 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.ejbLite-3.2; type="osgi.subsystem.feature"
```

### Features that this feature enables

- jndi-1.0 - Java Naming and Directory Interface

### Features that enable this feature

- ejb-3.2 - Enterprise JavaBeans 3.2
- ejbHome-3.2 - Enterprise JavaBeans Home Interfaces 3.2
- ejbPersistentTimer-3.2 - Enterprise JavaBeans Persistent Timers 3.2
- ejbRemote-3.2 - Enterprise JavaBeans Remote 3.2
- webProfile-7.0 - Java EE Web Profile 7.0
-  zosLocalAdapters-1.0 - z/OS Optimized Local Adapters

### IBM API packages provided by this feature

- com.ibm.websphere.ejbcontainer.mbean

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Enterprise JavaBeans Lite 3.2 feature:

- application

- applicationManager
- applicationMonitor
- classloading
- ejbApplication
- ejbContainer
- enterpriseApplication
- javaPermission
- library
- transaction
- webApplication

## Enterprise JavaBeans Persistent Timers 3.2

This feature enables the use of persistent timers in Enterprise JavaBeans.

### Enabling this feature

To enable the Enterprise JavaBeans Persistent Timers 3.2 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>ejbPersistentTimer-3.2</feature>
```

### Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Enterprise JavaBeans Persistent Timers 3.2 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.ejbPersistentTimer-3.2; type="osgi.subsystem.feature"
```

### Features that this feature enables

- ejbLite-3.2 - Enterprise JavaBeans Lite 3.2
- jdbc-4.1 - Java Database Connectivity 4.1
- jndi-1.0 - Java Naming and Directory Interface

### Features that enable this feature

- ejb-3.2 - Enterprise JavaBeans 3.2

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Enterprise JavaBeans Persistent Timers 3.2 feature:

- classloading
- databaseStore
- persistentExecutor
- transaction

## Enterprise JavaBeans Remote 3.2

This feature enables the use of remote interfaces in Enterprise JavaBeans.

## Enabling this feature

To enable the Enterprise JavaBeans Remote 3.2 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>ejbRemote-3.2</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Enterprise JavaBeans Remote 3.2 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.ejbRemote-3.2; type="osgi.subsystem.feature"
```

## Features that this feature enables

- `ejbLite-3.2` - Enterprise JavaBeans Lite 3.2

## Features that enable this feature

- `ejb-3.2` - Enterprise JavaBeans 3.2

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Enterprise JavaBeans Remote 3.2 feature:

- `channelfw`
- `classloading`
- `iiopEndpoint`
- `iiopServerPolicies`
- `orb`
- `tcpOptions`
- `transaction`

## Event Logging

Logs a record of events, such as JDBC requests and servlet requests, and their durations.

## Enabling this feature

To enable the Event Logging feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>eventLogging-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Event Logging feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.eventLogging-1.0; type="osgi.subsystem.feature"
```

## SPI packages provided by this feature

- `com.ibm.wsspi.event.logging`

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Event Logging feature:

- `eventLogging`

## Expression Language 3.0

This feature enables support for the Expression Language (EL) 3.0.

### Enabling this feature

To enable the Expression Language 3.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>el-3.0</feature>
```

### Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Expression Language 3.0 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.el-3.0; type="osgi.subsystem.feature"
```

### Features that enable this feature

- `beanValidation-1.1` - Bean Validation 1.1
- `jsp-2.3` - JavaServer Pages 2.3
- `webProfile-7.0` - Java EE Web Profile 7.0

### Standard API packages provided by this feature

- `javax.el`

## Federated User Registry

This feature enables support for federation of multiple user registries.

### Enabling this feature

To enable the Federated User Registry feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>federatedRegistry-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Federated User Registry feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.federatedRegistry-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- ssl-1.0 - Secure Socket Layer

### Features that enable this feature

- ldapRegistry-3.0 - LDAP User Registry
- scim-1.0 - System for Cross-domain Identity Management

### SPI packages provided by this feature

- com.ibm.wsspi.security.wim
- com.ibm.wsspi.security.wim.exception
- com.ibm.wsspi.security.wim.model

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Federated User Registry feature:

- federatedRepository

### Health Analyzer

The Health Analyzer feature provides health data collection for the Health Manager.

### Enabling this feature

To enable the Health Analyzer feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>healthAnalyzer-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Health Analyzer feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.health.healthAnalyzer-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- collectiveMember-1.0 - Collective Member
- json-1.0 - JavaScript Object Notation for Java
- restConnector-1.0 - JMX REST Connector 1.0
- restConnector-2.0 - JMX REST Connector 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Health Analyzer feature:

- channelfw
- classloading
- httpAccessLogging
- httpDispatcher
- httpEncoding
- httpEndpoint
- httpOptions

- httpProxyRedirect
- mimeTypes
- tcpOptions
- virtualHost

## Health Manager

The Health Manager feature provides health monitoring and automatic actions based on Health Policy.

### Enabling this feature

To enable the Health Manager feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>healthManager-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Health Manager feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.health.healthManager-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- collectiveController-1.0 - Collective Controller
- json-1.0 - JavaScript Object Notation for Java
- restConnector-1.0 - JMX REST Connector 1.0
- restConnector-2.0 - JMX REST Connector 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Health Manager feature:

- healthPolicy

## J2EE Management 1.1

This feature allows applications to utilize the interfaces defined in the JSR77 specification.

### Enabling this feature

To enable the J2EE Management 1.1 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>j2eeManagement-1.1</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the J2EE Management 1.1 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.j2eeManagement-1.1; type="osgi.subsystem.feature"
```

### Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0

## Standard API packages provided by this feature

- javax.management.j2ee
- javax.management.j2ee.statistics
- org.omg.stub.javax.management.j2ee

## IBM API packages provided by this feature

- com.ibm.websphere.management.j2ee

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the J2EE Management 1.1 feature:

- channelfw
- classloading
- orb
- tcpOptions
- transaction

## JMS 1.1 Client for IBM MQ

This feature provides applications with access to message queues hosted on WebSphere MQ through the JMS 1.1 API.

## Enabling this feature

To enable the JMS 1.1 Client for IBM MQ feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>wmqJmsClient-1.1</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the JMS 1.1 Client for IBM MQ feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.wmqJmsClient-1.1; type="osgi.subsystem.feature"
```

## Standard API packages provided by this feature

- javax.jms

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the JMS 1.1 Client for IBM MQ feature:

- activationSpec
- adminObject
- application
- applicationManager
- applicationMonitor
- authData

- classloading
- connectionFactory
- connectionManager
- javaPermission
- jmsActivationSpec
- jmsConnectionFactory
- jmsDestination
- jmsQueue
- jmsQueueConnectionFactory
- jmsTopic
- jmsTopicConnectionFactory
- library
- resourceAdapter
- transaction
- wmqJmsClient

## **JMS 1.1 Client for Message Server**

This feature provides applications with access to message queues hosted on WebSphere Application Server through the JMS 1.1 API. It enables access both to the messaging engine enabled via the wasJmsServer feature, and to a service integration bus hosted in a full profile server.

### **Enabling this feature**

To enable the JMS 1.1 Client for Message Server feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>wasJmsClient-1.1</feature>
```

### **Supported Java Versions**

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the JMS 1.1 Client for Message Server feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.wasJmsClient-1.1; type="osgi.subsystem.feature"
```

### **Standard API packages provided by this feature**

- javax.jms

### **Feature configuration elements**

You can use the following elements in your server.xml file to configure the JMS 1.1 Client for Message Server feature:

- activationSpec
- adminObject
- application
- applicationManager
- applicationMonitor

- authData
- channelfw
- classloading
- connectionFactory
- connectionManager
- javaPermission
- jmsActivationSpec
- jmsConnectionFactory
- jmsDestination
- jmsQueue
- jmsQueueConnectionFactory
- jmsTopic
- jmsTopicConnectionFactory
- library
- resourceAdapter
- tcpOptions
- transaction
- wasJmsOutbound

## **JMS 2.0 Client for IBM MQ**

This feature provides applications with access to message queues hosted on IBM MQ through the JMS 2.0 API.

### **Enabling this feature**

To enable the JMS 2.0 Client for IBM MQ feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>wmqJmsClient-2.0</feature>
```

### **Supported Java Versions**

- JavaSE-1.7
- JavaSE-1.8

### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the JMS 2.0 Client for IBM MQ feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.wmqJmsClient-2.0; type="osgi.subsystem.feature"
```

### **Feature configuration elements**

You can use the following elements in your server.xml file to configure the JMS 2.0 Client for IBM MQ feature:

- activationSpec
- adminObject
- application
- applicationManager
- applicationMonitor
- authData

- classloading
- connectionFactory
- connectionManager
- javaPermission
- jmsActivationSpec
- jmsConnectionFactory
- jmsDestination
- jmsQueue
- jmsQueueConnectionFactory
- jmsTopic
- jmsTopicConnectionFactory
- library
- resourceAdapter
- transaction
- wmqJmsClient

## JMS 2.0 Client for Message Server

The wasJmsClient-2.0 feature provides applications with access to the message queues that are hosted on WebSphere Application Server through the JMS 2.0 API. This feature supersedes wasJmsClient-1.1. The wasJmsClient-2.0 feature is compliant with JMS 2.0 specifications and is supported only on JDK 7 or later. It enables access to the messaging engine that is enabled through the wasJmsServer feature, and also to the service integration bus that is hosted on a full profile server.

### Enabling this feature

To enable the JMS 2.0 Client for Message Server feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>wasJmsClient-2.0</feature>
```

### Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the JMS 2.0 Client for Message Server feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.wasJmsClient-2.0; type="osgi.subsystem.feature"
```

### Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0
- javaeeClient-7.0 - Java EE V7 Application Client

### Standard API packages provided by this feature

- javax.jms

### Feature configuration elements

You can use the following elements in your server.xml file to configure the JMS 2.0 Client for Message Server feature:

- activationSpec

- adminObject
- application
- applicationManager
- applicationMonitor
- authData
- channelfw
- classloading
- connectionFactory
- connectionManager
- javaPermission
- jmsActivationSpec
- jmsConnectionFactory
- jmsDestination
- jmsQueue
- jmsQueueConnectionFactory
- jmsTopic
- jmsTopicConnectionFactory
- library
- resourceAdapter
- tcpOptions
- transaction
- wasJmsOutbound

### **JMS Message-Driven Beans 3.1**

This feature enables the use of JMS Message-Driven Enterprise JavaBeans written to the EJB 3.1 specification. MDBs allow asynchronous processing of messages within a Java EE component.

#### **Enabling this feature**

To enable the JMS Message-Driven Beans 3.1 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jmsMdb-3.1</feature>
```

#### **Supported Java Versions**

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

#### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the JMS Message-Driven Beans 3.1 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jmsMdb-3.1; type="osgi.subsystem.feature"
```

#### **Features that this feature is superseded by**

- mdb-3.1 - Message-Driven Beans 3.1

### Features that this feature enables

- jca-1.6 - Java Connector Architecture 1.6
- jndi-1.0 - Java Naming and Directory Interface

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the JMS Message-Driven Beans 3.1 feature:

- application
- applicationManager
- applicationMonitor
- classloading
- ejbApplication
- ejbContainer
- enterpriseApplication
- javaPermission
- library
- transaction
- webApplication

### JMS Message-Driven Beans 3.2

This feature is superseded by `mdb-3.2`. Both features provide identical function; only the feature names are different. `mdb-3.2` is the preferred feature name.

### Enabling this feature

To enable the JMS Message-Driven Beans 3.2 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>jmsMdb-3.2</feature>
```

### Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the JMS Message-Driven Beans 3.2 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jmsMdb-3.2; type="osgi.subsystem.feature"
```

### Features that this feature is superseded by

- `mdb-3.2` - Message-Driven Beans 3.2

### Features that this feature enables

- `mdb-3.2` - Message-Driven Beans 3.2

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the JMS Message-Driven Beans 3.2 feature:

- classloading

- transaction

## JMX Local Connector

This feature allows the use of a local JMX connector that is built into the JVM to access JMX resources in the server. The JMX connector can only be used on the same host machine by a client that has the same user ID and the same JDK as the server process. It enables local access by JMX clients such as jConsole, or other JMX clients that use the Attach API.

### Enabling this feature

To enable the JMX Local Connector feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>localConnector-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the JMX Local Connector feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.localConnector-1.0; type="osgi.subsystem.feature"
```

## JMX REST Connector 1.0

A secure JMX connector that can be used locally or remotely using any JDK. It enables remote access by JMX clients via a REST-based connector and requires SSL and basic user security configuration. This feature is superseded by the restConnector-2.0 feature. This feature enables the jaxrs-1.1 feature.

### Enabling this feature

To enable the JMX REST Connector 1.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>restConnector-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the JMX REST Connector 1.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.restConnector-1.0; type="osgi.subsystem.feature"
```

### Features that this feature is superseded by

- jaxrs-1.1 - Java RESTful Services 1.1
- json-1.0 - JavaScript Object Notation for Java
- restConnector-2.0 - JMX REST Connector 2.0

### Features that this feature enables

- distributedMap-1.0 - Distributed Map interface for Dynamic Caching
- json-1.0 - JavaScript Object Notation for Java
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1
- ssl-1.0 - Secure Socket Layer

## Features that enable this feature

- adminCenter-1.0 - Admin Center
- clusterMember-1.0 - Static Cluster Member
- collectiveController-1.0 - Collective Controller
- collectiveMember-1.0 - Collective Member
- dynamicRouting-1.0 - Dynamic Routing
- healthAnalyzer-1.0 - Health Analyzer
- healthManager-1.0 - Health Manager
- scalingController-1.0 - Scaling Controller
- scalingMember-1.0 - Scaling Member

## IBM API packages provided by this feature

- com.ibm.websphere.filetransfer
- com.ibm.websphere.jmx.connector.rest
- com.ibm.ws.jmx.connector.client.rest

## SPI packages provided by this feature

- com.ibm.wsspi.collective.plugins
- com.ibm.wsspi.collective.plugins.helpers

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the JMX REST Connector 1.0 feature:

- administrator-role
- authCache
- authentication
- authorization-roles
- basicRegistry
- channelfw
- classloading
- httpAccessLogging
- httpDispatcher
- httpEncoding
- httpEndpoint
- httpOptions
- httpProxyRedirect
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- mimeTypees
- quickStartSecurity
- remoteFileAccess
- tcpOptions
- trustAssociation
- virtualHost

## JMX REST Connector 2.0

A secure JMX connector that can be used locally or remotely using any JDK. It enables remote access by JMX clients via a REST-based connector and requires SSL and basic user security configuration. This feature supersedes the restConnector-1.0 feature and does not include the jaxrs-1.1 feature.

### Enabling this feature

To enable the JMX REST Connector 2.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>restConnector-2.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the JMX REST Connector 2.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.restConnector-2.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- distributedMap-1.0 - Distributed Map interface for Dynamic Caching
- json-1.0 - JavaScript Object Notation for Java
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1
- ssl-1.0 - Secure Socket Layer

### Features that enable this feature

- adminCenter-1.0 - Admin Center
- clusterMember-1.0 - Static Cluster Member
- collectiveController-1.0 - Collective Controller
- collectiveMember-1.0 - Collective Member
- dynamicRouting-1.0 - Dynamic Routing
- healthAnalyzer-1.0 - Health Analyzer
- healthManager-1.0 - Health Manager
- scalingController-1.0 - Scaling Controller
- scalingMember-1.0 - Scaling Member

### IBM API packages provided by this feature

- com.ibm.websphere.filetransfer
- com.ibm.websphere.jmx.connector.rest
- com.ibm.ws.jmx.connector.client.rest

### SPI packages provided by this feature

- com.ibm.wsspi.collective.plugins
- com.ibm.wsspi.collective.plugins.helpers

### Feature configuration elements

You can use the following elements in your server.xml file to configure the JMX REST Connector 2.0 feature:

- administrator-role
- authCache

- authentication
- authorization-roles
- basicRegistry
- channelfw
- classloading
- httpAccessLogging
- httpDispatcher
- httpEncoding
- httpEndpoint
- httpOptions
- httpProxyRedirect
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- mimeTypees
- quickStartSecurity
- remoteFileAccess
- tcpOptions
- trustAssociation
- virtualHost

## Java Authentication SPI for Containers 1.1

This feature enables support for securing the server runtime environment and applications using Java Authentication SPI for Containers (JASPIC) providers as defined in JSR-196

### Enabling this feature

To enable the Java Authentication SPI for Containers 1.1 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jaspic-1.1</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Authentication SPI for Containers 1.1 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jaspic-1.1; type="osgi.subsystem.feature"
```

### Features that this feature enables

- appSecurity-2.0 - Application Security 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0

## Standard API packages provided by this feature

- javax.security.auth.message
- javax.security.auth.message.callback
- javax.security.auth.message.config
- javax.security.auth.message.module

## SPI packages provided by this feature

- com.ibm.wsspi.security.jaspi

## Java Authorization Contract for Containers 1.5

This feature enables support for Java Authorization Contract for Containers (JACC) version 1.5. In order to add the jacc-1.5 feature to your server, you need to add the third party JACC provider which is not a part of the WebSphere Application Server Liberty profile.

## Enabling this feature

To enable the Java Authorization Contract for Containers 1.5 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jacc-1.5</feature>
```

## Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Authorization Contract for Containers 1.5 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jacc-1.5; type="osgi.subsystem.feature"
```

## Features that this feature enables

- appSecurity-2.0 - Application Security 2.0

## Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0

## Standard API packages provided by this feature

- javax.security.jacc

## IBM API packages provided by this feature

- com.ibm.wsspi.security.authorization.jacc

## Feature configuration elements

You can use the following elements in your server.xml file to configure the Java Authorization Contract for Containers 1.5 feature:

- classloading

## Java Connector Architecture 1.0 Security Inflow

This feature enables security inflow for resource adapters.

## Enabling this feature

To enable the Java Connector Architecture 1.0 Security Inflow feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jcaInboundSecurity-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Connector Architecture 1.0 Security Inflow feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jcaInboundSecurity-1.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- jca-1.6 - Java Connector Architecture 1.6
- jca-1.7 - Java Connector Architecture 1.7
- ssl-1.0 - Secure Socket Layer

## Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0

## Standard API packages provided by this feature

- javax.security.auth.message.callback

## Feature configuration elements

You can use the following elements in your server.xml file to configure the Java Connector Architecture 1.0 Security Inflow feature:

- administrator-role
- authCache
- authentication
- basicRegistry
- classloading
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- quickStartSecurity
- transaction

## Java Connector Architecture 1.6

This feature enables the configuration of resource adapters to access Enterprise Information Systems (EIS) from applications. The configuration of a resource adapter also includes the configuration of connection factories, administered objects and activation specifications. Any resource adapter that complies with the JCA 1.6 specification can be used. High performance connection pooling is also provided.

## Enabling this feature

To enable the Java Connector Architecture 1.6 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jca-1.6</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Connector Architecture 1.6 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jca-1.6; type="osgi.subsystem.feature"
```

## Features that enable this feature

- jcaInboundSecurity-1.0 - Java Connector Architecture 1.0 Security Inflow
- jms-1.1 - Java Message Service 1.1
- jmsMdb-3.1 - JMS Message-Driven Beans 3.1
- mdb-3.1 - Message-Driven Beans 3.1
-  zosLocalAdapters-1.0 - z/OS Optimized Local Adapters

## Feature configuration elements

You can use the following elements in your server.xml file to configure the Java Connector Architecture 1.6 feature:

- activationSpec
- adminObject
- application
- applicationManager
- applicationMonitor
- authData
- classloading
- connectionFactory
- connectionManager
- javaPermission
- library
- resourceAdapter
- transaction

## Java Connector Architecture 1.7

This feature enables the configuration of resource adapters to access Enterprise Information Systems (EIS) from applications. The configuration of a resource adapter also includes the configuration of connection factories, administered objects and activation specifications. Any resource adapter that complies with the JCA 1.7 specification or lower can be used. High performance connection pooling is also provided.

## Enabling this feature

To enable the Java Connector Architecture 1.7 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jca-1.7</feature>
```

## Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Connector Architecture 1.7 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jca-1.7; type="osgi.subsystem.feature"
```

## Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0
- jcaInboundSecurity-1.0 - Java Connector Architecture 1.0 Security Inflow
- jms-2.0 - Java Message Service 2.0
- mdb-3.2 - Message-Driven Beans 3.2
-  zosLocalAdapters-1.0 - z/OS Optimized Local Adapters

## Feature configuration elements

You can use the following elements in your server.xml file to configure the Java Connector Architecture 1.7 feature:

- activationSpec
- adminObject
- application
- applicationManager
- applicationMonitor
- authData
- classloading
- connectionFactory
- connectionManager
- javaPermission
- library
- resourceAdapter
- transaction

## Java Database Connectivity 4.0

This feature enables the configuration of DataSources to access Databases from applications. Any database that complies with the JDBC 4.0 specification can be used; customized configuration of many specific providers is included. High performance connection pooling is also provided.

## Enabling this feature

To enable the Java Database Connectivity 4.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jdbc-4.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Database Connectivity 4.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jdbc-4.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- jndi-1.0 - Java Naming and Directory Interface

### Features that enable this feature

- batch-1.0 - Batch API 1.0
- batchManagement-1.0 - Batch Management
- jpa-2.0 - Java Persistence API 2.0
- osgi.jpa-1.0 - OSGi Java Persistence API
- sessionDatabase-1.0 - Database Session Persistence
- webProfile-6.0 - Java EE Web Profile 6.0

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java Database Connectivity 4.0 feature:

- `authData`
- `classloading`
- `connectionManager`
- `dataSource`
- `jdbcDriver`
- `library`
- `transaction`

### Java Database Connectivity 4.1

This feature enables the configuration of `DataSources` to access Databases from applications. Any JDBC driver that complies with the JDBC 4.1, 4.0, 3.0, or 2.x specification can be used; customized configuration of many specific providers is included. High performance connection pooling is also provided.

### Enabling this feature

To enable the Java Database Connectivity 4.1 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>jdbc-4.1</feature>
```

### Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Database Connectivity 4.1 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jdbc-4.1; type="osgi.subsystem.feature"
```

## Features that enable this feature

- batch-1.0 - Batch API 1.0
- batchManagement-1.0 - Batch Management
- ejbPersistentTimer-3.2 - Enterprise JavaBeans Persistent Timers 3.2
- javaeeClient-7.0 - Java EE V7 Application Client
- jpa-2.0 - Java Persistence API 2.0
- jpa-2.1 - Java Persistence API 2.1
- osgi.jpa-1.0 - OSGi Java Persistence API
- sessionDatabase-1.0 - Database Session Persistence
- webProfile-6.0 - Java EE Web Profile 6.0
- webProfile-7.0 - Java EE Web Profile 7.0

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java Database Connectivity 4.1 feature:

- authData
- classloading
- connectionManager
- dataSource
- jdbcDriver
- library
- transaction

## Java EE Full Platform 7.0

This feature combines the Liberty features that support the Java EE 7.0 Full Platform.

## Enabling this feature

To enable the Java EE Full Platform 7.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>javaee-7.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Java EE Full Platform 7.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.javaee-7.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- appClientSupport-1.0 - Application Client Support for Server
- batch-1.0 - Batch API 1.0
- concurrent-1.0 - Concurrency Utilities for Java EE 1.0
- ejb-3.2 - Enterprise JavaBeans 3.2

- j2eeManagement-1.1 - J2EE Management 1.1
- jacc-1.5 - Java Authorization Contract for Containers 1.5
- jaspic-1.1 - Java Authentication SPI for Containers 1.1
- javaMail-1.5 - JavaMail 1.5
- jaxws-2.2 - Java Web Services 2.2
- jca-1.7 - Java Connector Architecture 1.7
- jcaInboundSecurity-1.0 - Java Connector Architecture 1.0 Security Inflow
- servlet-3.1 - Java Servlets 3.1
- wasJmsClient-2.0 - JMS 2.0 Client for Message Server
- wasJmsSecurity-1.0 - Message Server Security 1.0
- wasJmsServer-1.0 - Message Server 1.0
- webProfile-7.0 - Java EE Web Profile 7.0

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java EE Full Platform 7.0 feature:

- `classloading`
- `transaction`

### Java EE Managed Bean 1.0

This feature enables support for the Managed Beans 1.0 specification. Managed Beans provide a common foundation for different Java EE components types that are managed by a container. Common services provided to Managed Beans include resource injection, lifecycle management and the use of interceptors.

### Enabling this feature

To enable the Java EE Managed Bean 1.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>managedBeans-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java EE Managed Bean 1.0 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.managedBeans-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `jndi-1.0` - Java Naming and Directory Interface

### Features that enable this feature

- `javaeeClient-7.0` - Java EE V7 Application Client
- `webProfile-6.0` - Java EE Web Profile 6.0
- `webProfile-7.0` - Java EE Web Profile 7.0

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java EE Managed Bean 1.0 feature:

- `classloading`
- `ejbContainer`
- `library`
- `transaction`

## Java EE V7 Application Client

This feature enables support for Java EE 7 Application Client.

### Enabling this feature

To enable the Java EE V7 Application Client feature, add the following element declaration inside the `featureManager` element in your `client.xml` file:

```
<feature>javaeeClient-7.0</feature>
```

### Features that this feature enables

- `beanValidation-1.1` - Bean Validation 1.1
- `cdi-1.2` - Contexts and Dependency Injection 1.2
- `javaMail-1.5` - JavaMail 1.5
- `jaxb-2.2` - Java XML Bindings 2.2
- `jdbc-4.1` - Java Database Connectivity 4.1
- `jndi-1.0` - Java Naming and Directory Interface
- `jpa-2.1` - Java Persistence API 2.1
- `jsonp-1.0` - JavaScript Object Notation Processing
- `managedBeans-1.0` - Java EE Managed Bean 1.0
- `wasJmsClient-2.0` - JMS 2.0 Client for Message Server

## Feature configuration elements

You can use the following elements in your `client.xml` file to configure the Java EE V7 Application Client feature:

- `application`
- `applicationManager`
- `applicationMonitor`
- `channelfw`
- `classloading`
- `ejbApplication`
- `ejbContainer`
- `enterpriseApplication`
- `javaPermission`
- `library`
- `orb`
- `tcpOptions`
- `transaction`
- `webApplication`

## Java EE Web Profile 6.0

This feature provides a convenient combination of the Liberty features that are required to support the Java EE Web Profile.

### Enabling this feature

To enable the Java EE Web Profile 6.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>webProfile-6.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java EE Web Profile 6.0 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.webProfile-6.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `appSecurity-2.0` - Application Security 2.0
- `beanValidation-1.0` - Bean Validation 1.0
- `cdi-1.0` - Contexts and Dependency Injection 1.0
- `ejbLite-3.1` - Enterprise JavaBeans Lite 3.1
- `jdbc-4.0` - Java Database Connectivity 4.0
- `jdbc-4.1` - Java Database Connectivity 4.1
- `jndi-1.0` - Java Naming and Directory Interface
- `jpa-2.0` - Java Persistence API 2.0
- `jsf-2.0` - JavaServer Faces 2.0
- `jsp-2.2` - JavaServer Pages 2.2
- `managedBeans-1.0` - Java EE Managed Bean 1.0
- `servlet-3.0` - Java Servlets 3.0

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java EE Web Profile 6.0 feature:

- `classloading`
- `transaction`

## Java EE Web Profile 7.0

This feature combines the Liberty features that support the Java EE 7.0 Web Profile.

### Enabling this feature

To enable the Java EE Web Profile 7.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>webProfile-7.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java EE Web Profile 7.0 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.webProfile-7.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- appSecurity-2.0 - Application Security 2.0
- beanValidation-1.1 - Bean Validation 1.1
- cdi-1.2 - Contexts and Dependency Injection 1.2
- ejbLite-3.2 - Enterprise JavaBeans Lite 3.2
- el-3.0 - Expression Language 3.0
- jaxrs-2.0 - Java RESTful Services 2.0
- jdbc-4.1 - Java Database Connectivity 4.1
- jndi-1.0 - Java Naming and Directory Interface
- jpa-2.1 - Java Persistence API 2.1
- jsf-2.2 - JavaServer Faces 2.2
- jsonp-1.0 - JavaScript Object Notation Processing
- jsp-2.3 - JavaServer Pages 2.3
- managedBeans-1.0 - Java EE Managed Bean 1.0
- servlet-3.1 - Java Servlets 3.1
- websocket-1.1 - Java WebSocket 1.1

## Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java EE Web Profile 7.0 feature:

- classloading
- transaction

## Java Message Service 1.1

This feature enables the configuration of resource adapters to access messaging systems using the Java Message Service API. This also includes the configuration JMS connection factories, queues, topics and activation specifications. Any JMS resource adapter that complies with the JCA 1.6 specification can be used.

## Enabling this feature

To enable the Java Message Service 1.1 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>jms-1.1</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Message Service 1.1 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jms-1.1; type="osgi.subsystem.feature"
```

## Features that this feature enables

- jca-1.6 - Java Connector Architecture 1.6

## Standard API packages provided by this feature

- javax.jms

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java Message Service 1.1 feature:

- activationSpec
- adminObject
- application
- applicationManager
- applicationMonitor
- authData
- classloading
- connectionFactory
- connectionManager
- javaPermission
- jmsActivationSpec
- jmsConnectionFactory
- jmsDestination
- jmsQueue
- jmsQueueConnectionFactory
- jmsTopic
- jmsTopicConnectionFactory
- library
- resourceAdapter
- transaction

## Java Message Service 2.0

This feature enables the configuration of resource adapters to access messaging systems using the Java Message Service API. This also includes the configuration JMS connection factories, queues, topics and activation specifications. Any JMS resource adapter that complies with the JCA 1.7 specification can be used.

## Enabling this feature

To enable the Java Message Service 2.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>jms-2.0</feature>
```

## Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Message Service 2.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jms-2.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- jca-1.7 - Java Connector Architecture 1.7

## Standard API packages provided by this feature

- javax.jms

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java Message Service 2.0 feature:

- activationSpec
- adminObject
- application
- applicationManager
- applicationMonitor
- authData
- classloading
- connectionFactory
- connectionManager
- javaPermission
- jmsActivationSpec
- jmsConnectionFactory
- jmsDestination
- jmsQueue
- jmsQueueConnectionFactory
- jmsTopic
- jmsTopicConnectionFactory
- library
- resourceAdapter
- transaction

## Java Naming and Directory Interface

This feature enables the use of Java Naming and Directory Interface (JNDI) to access server configured resources such as DataSources or JMS Connection Factories. It also allows access to Java primitives configured in the server as a `jndiEntry`.

## Enabling this feature

To enable the Java Naming and Directory Interface feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>jndi-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Naming and Directory Interface feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jndi-1.0; type="osgi.subsystem.feature"
```

## Features that enable this feature

- appClientSupport-1.0 - Application Client Support for Server
- batch-1.0 - Batch API 1.0
- distributedMap-1.0 - Distributed Map interface for Dynamic Caching
- ejbLite-3.1 - Enterprise JavaBeans Lite 3.1
- ejbLite-3.2 - Enterprise JavaBeans Lite 3.2
- ejbPersistentTimer-3.2 - Enterprise JavaBeans Persistent Timers 3.2
- javaeeClient-7.0 - Java EE V7 Application Client
- jdbc-4.0 - Java Database Connectivity 4.0
- jmsMdb-3.1 - JMS Message-Driven Beans 3.1
- jpa-2.0 - Java Persistence API 2.0
- jpa-2.1 - Java Persistence API 2.1
- managedBeans-1.0 - Java EE Managed Bean 1.0
- mdb-3.1 - Message-Driven Beans 3.1
- mdb-3.2 - Message-Driven Beans 3.2
- osgi.jpa-1.0 - OSGi Java Persistence API
- sessionDatabase-1.0 - Database Session Persistence
- webProfile-6.0 - Java EE Web Profile 6.0
- webProfile-7.0 - Java EE Web Profile 7.0
-  zosLocalAdapters-1.0 - z/OS Optimized Local Adapters
-  zosRequestLogging-1.0 - z/OS Request Logging

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java Naming and Directory Interface feature:

- classloading
- jndiEntry
- jndiObjectFactory
- jndiReferenceEntry
- jndiURLEntry
- library

## Java Persistence API 2.0

This feature enables support for applications that use application-managed and container-managed JPA written to the Java Persistence API 2.0 specification. The support is built on top of Apache OpenJPA with extensions to support the container-managed programming model.

## Enabling this feature

To enable the Java Persistence API 2.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jpa-2.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Persistence API 2.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jpa-2.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- beanValidation-1.0 - Bean Validation 1.0
- beanValidation-1.1 - Bean Validation 1.1
- jdbc-4.0 - Java Database Connectivity 4.0
- jdbc-4.1 - Java Database Connectivity 4.1
- jndi-1.0 - Java Naming and Directory Interface
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

## Features that enable this feature

- osgi.jpaa-1.0 - OSGi Java Persistence API
- webProfile-6.0 - Java EE Web Profile 6.0

## Standard API packages provided by this feature

- javax.persistence
- javax.persistence.criteria
- javax.persistence.metamodel
- javax.persistence.spi

## Third party API packages provided by this feature

- org.apache.openjpa.abstractstore
- org.apache.openjpa.ant
- org.apache.openjpa.audit
- org.apache.openjpa.conf
- org.apache.openjpa.datacache
- org.apache.openjpa.ee
- org.apache.openjpa.enhance
- org.apache.openjpa.event
- org.apache.openjpa.instrumentation
- org.apache.openjpa.instrumentation.jmx
- org.apache.openjpa.jdbc.ant
- org.apache.openjpa.jdbc.conf
- org.apache.openjpa.jdbc.identifier
- org.apache.openjpa.jdbc.kernel
- org.apache.openjpa.jdbc.kernel.exps
- org.apache.openjpa.jdbc.meta

- org.apache.openjpa.jdbc.meta.strats
- org.apache.openjpa.jdbc.schema
- org.apache.openjpa.jdbc.sql
- org.apache.openjpa.kernel
- org.apache.openjpa.kernel.exps
- org.apache.openjpa.kernel.jpql
- org.apache.openjpa.lib.ant
- org.apache.openjpa.lib.conf
- org.apache.openjpa.lib.encryption
- org.apache.openjpa.lib.graph
- org.apache.openjpa.lib.identifier
- org.apache.openjpa.lib.instrumentation
- org.apache.openjpa.lib.jdbc
- org.apache.openjpa.lib.log
- org.apache.openjpa.lib.meta
- org.apache.openjpa.lib.rop
- org.apache.openjpa.lib.util
- org.apache.openjpa.lib.util.concurrent
- org.apache.openjpa.lib.util.svn
- org.apache.openjpa.lib.xml
- org.apache.openjpa.meta
- org.apache.openjpa.persistence
- org.apache.openjpa.persistence.criteria
- org.apache.openjpa.persistence.jdbc
- org.apache.openjpa.persistence.meta
- org.apache.openjpa.persistence.osgi
- org.apache.openjpa.persistence.query
- org.apache.openjpa.persistence.util
- org.apache.openjpa.persistence.validation
- org.apache.openjpa.slice
- org.apache.openjpa.slice.jdbc
- org.apache.openjpa.util
- org.apache.openjpa.validation
- org.apache.openjpa.xmlstore

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java Persistence API 2.0 feature:

- classloading
- jpa
- library
- transaction

## Java Persistence API 2.1

This feature enables support for applications that use application-managed and container-managed JPA written to the Java Persistence API 2.1 specification. The support is built on top of EclipseLink to support the container-managed programming model.

### Enabling this feature

To enable the Java Persistence API 2.1 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jpa-2.1</feature>
```

### Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Persistence API 2.1 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jpa-2.1; type="osgi.subsystem.feature"
```

### Features that this feature enables

- jdbc-4.1 - Java Database Connectivity 4.1
- jndi-1.0 - Java Naming and Directory Interface

### Features that enable this feature

- javaeeClient-7.0 - Java EE V7 Application Client
- webProfile-7.0 - Java EE Web Profile 7.0

### Standard API packages provided by this feature

- javax.persistence
- javax.persistence.criteria
- javax.persistence.metamodel
- javax.persistence.spi

### Third party API packages provided by this feature

- org.eclipse.persistence
- org.eclipse.persistence.annotations
- org.eclipse.persistence.config
- org.eclipse.persistence.core.descriptors
- org.eclipse.persistence.core.mappings
- org.eclipse.persistence.core.mappings.converters
- org.eclipse.persistence.core.queries
- org.eclipse.persistence.core.sessions
- org.eclipse.persistence.descriptors
- org.eclipse.persistence.descriptors.copying
- org.eclipse.persistence.descriptors.invalidation
- org.eclipse.persistence.descriptors.partitioning
- org.eclipse.persistence.dynamic

- org.eclipse.persistence.eis
- org.eclipse.persistence.eis.interactions
- org.eclipse.persistence.eis.mappings
- org.eclipse.persistence.exceptions
- org.eclipse.persistence.exceptions.i18n
- org.eclipse.persistence.expressions
- org.eclipse.persistence.expressions.spatial
- org.eclipse.persistence.history
- org.eclipse.persistence.internal.cache
- org.eclipse.persistence.internal.codegen
- org.eclipse.persistence.internal.core.databaseaccess
- org.eclipse.persistence.internal.core.descriptors
- org.eclipse.persistence.internal.core.helper
- org.eclipse.persistence.internal.core.queries
- org.eclipse.persistence.internal.core.sessions
- org.eclipse.persistence.internal.databaseaccess
- org.eclipse.persistence.internal.descriptors.changetracking
- org.eclipse.persistence.internal.dynamic
- org.eclipse.persistence.internal.expressions
- org.eclipse.persistence.internal.helper
- org.eclipse.persistence.internal.helper.linkedlist
- org.eclipse.persistence.internal.history
- org.eclipse.persistence.internal.indirection
- org.eclipse.persistence.internal.jpa
- org.eclipse.persistence.internal.jpa.deployment
- org.eclipse.persistence.internal.jpa.deployment.xml.parser
- org.eclipse.persistence.internal.jpa.jdbc
- org.eclipse.persistence.internal.jpa.jpql
- org.eclipse.persistence.internal.jpa.metadata
- org.eclipse.persistence.internal.jpa.metadata.accessors
- org.eclipse.persistence.internal.jpa.metadata.accessors.classes
- org.eclipse.persistence.internal.jpa.metadata.accessors.mappings
- org.eclipse.persistence.internal.jpa.metadata.accessors.objects
- org.eclipse.persistence.internal.jpa.metadata.additionalcriteria
- org.eclipse.persistence.internal.jpa.metadata.cache
- org.eclipse.persistence.internal.jpa.metadata.changetracking
- org.eclipse.persistence.internal.jpa.metadata.columns
- org.eclipse.persistence.internal.jpa.metadata.converters
- org.eclipse.persistence.internal.jpa.metadata.copypolicy
- org.eclipse.persistence.internal.jpa.metadata.inheritance
- org.eclipse.persistence.internal.jpa.metadata.listeners
- org.eclipse.persistence.internal.jpa.metadata.locking
- org.eclipse.persistence.internal.jpa.metadata.mappings
- org.eclipse.persistence.internal.jpa.metadata.multitenant
- org.eclipse.persistence.internal.jpa.metadata.nosql

- org.eclipse.persistence.internal.jpa.metadata.partitioning
- org.eclipse.persistence.internal.jpa.metadata.queries
- org.eclipse.persistence.internal.jpa.metadata.sequencing
- org.eclipse.persistence.internal.jpa.metadata.structures
- org.eclipse.persistence.internal.jpa.metadata.tables
- org.eclipse.persistence.internal.jpa.metadata.transformers
- org.eclipse.persistence.internal.jpa.metadata.xml
- org.eclipse.persistence.internal.jpa.metamodel
- org.eclipse.persistence.internal.jpa.parsing
- org.eclipse.persistence.internal.jpa.parsing.jpql
- org.eclipse.persistence.internal.jpa.parsing.jpql antlr
- org.eclipse.persistence.internal.jpa.querydef
- org.eclipse.persistence.internal.jpa.transaction
- org.eclipse.persistence.internal.jpa.weaving
- org.eclipse.persistence.internal.libraries.antlr.runtime
- org.eclipse.persistence.internal.libraries.antlr.runtime.debug
- org.eclipse.persistence.internal.libraries.antlr.runtime.misc
- org.eclipse.persistence.internal.libraries.antlr.runtime.tree
- org.eclipse.persistence.internal.libraries.asm
- org.eclipse.persistence.internal.libraries.asm.common
- org.eclipse.persistence.internal.libraries.asm.signature
- org.eclipse.persistence.internal.libraries.asm.tree
- org.eclipse.persistence.internal.libraries.asm.tree.analysis
- org.eclipse.persistence.internal.libraries.asm.util
- org.eclipse.persistence.internal.libraries.asm.xml
- org.eclipse.persistence.internal.localization
- org.eclipse.persistence.internal.localization.i18n
- org.eclipse.persistence.internal.oxm
- org.eclipse.persistence.internal.oxm.accessor
- org.eclipse.persistence.internal.oxm.conversion
- org.eclipse.persistence.internal.oxm.documentpreservation
- org.eclipse.persistence.internal.oxm.mappings
- org.eclipse.persistence.internal.oxm.record
- org.eclipse.persistence.internal.oxm.record.deferred
- org.eclipse.persistence.internal.oxm.record.json
- org.eclipse.persistence.internal.oxm.record.namespaces
- org.eclipse.persistence.internal.oxm.schema
- org.eclipse.persistence.internal.oxm.schema.model
- org.eclipse.persistence.internal.oxm.unmapped
- org.eclipse.persistence.internal.platform.database
- org.eclipse.persistence.internal.queries
- org.eclipse.persistence.internal.security
- org.eclipse.persistence.internal.sequencing
- org.eclipse.persistence.internal.sessions
- org.eclipse.persistence.internal.sessions.coordination

- org.eclipse.persistence.internal.sessions.coordination.broadcast
- org.eclipse.persistence.internal.sessions.coordination.corba
- org.eclipse.persistence.internal.sessions.coordination.corba.sun
- org.eclipse.persistence.internal.sessions.coordination.jms
- org.eclipse.persistence.internal.sessions.coordination.rmi
- org.eclipse.persistence.internal.sessions.coordination.rmi.iiop
- org.eclipse.persistence.internal.sessions.factories
- org.eclipse.persistence.internal.sessions.factories.model
- org.eclipse.persistence.internal.sessions.factories.model.event
- org.eclipse.persistence.internal.sessions.factories.model.log
- org.eclipse.persistence.internal.sessions.factories.model.login
- org.eclipse.persistence.internal.sessions.factories.model.platform
- org.eclipse.persistence.internal.sessions.factories.model.pool
- org.eclipse.persistence.internal.sessions.factories.model.project
- org.eclipse.persistence.internal.sessions.factories.model.property
- org.eclipse.persistence.internal.sessions.factories.model.rcm
- org.eclipse.persistence.internal.sessions.factories.model.rcm.command
- org.eclipse.persistence.internal.sessions.factories.model.sequencing
- org.eclipse.persistence.internal.sessions.factories.model.session
- org.eclipse.persistence.internal.sessions.factories.model.transport
- org.eclipse.persistence.internal.sessions.factories.model.transport.discovery
- org.eclipse.persistence.internal.sessions.factories.model.transport.naming
- org.eclipse.persistence.internal.sessions.remote
- org.eclipse.persistence.jpa.dynamic
- org.eclipse.persistence.jpa.jpql
- org.eclipse.persistence.jpa.jpql.parser
- org.eclipse.persistence.jpa.jpql.tools
- org.eclipse.persistence.jpa.jpql.tools.model
- org.eclipse.persistence.jpa.jpql.tools.model.query
- org.eclipse.persistence.jpa.jpql.tools.resolver
- org.eclipse.persistence.jpa.jpql.tools.spi
- org.eclipse.persistence.jpa.jpql.tools.utility
- org.eclipse.persistence.jpa.jpql.tools.utility.filter
- org.eclipse.persistence.jpa.jpql.tools.utility.iterable
- org.eclipse.persistence.jpa.jpql.tools.utility.iterator
- org.eclipse.persistence.jpa.jpql.utility
- org.eclipse.persistence.jpa.jpql.utility.filter
- org.eclipse.persistence.jpa.jpql.utility.iterable
- org.eclipse.persistence.jpa.jpql.utility.iterator
- org.eclipse.persistence.jpa.metadata
- org.eclipse.persistence.logging
- org.eclipse.persistence.mappings
- org.eclipse.persistence.mappings.converters
- org.eclipse.persistence.mappings.foundation
- org.eclipse.persistence.mappings.querykeys

- org.eclipse.persistence.mappings.structures
- org.eclipse.persistence.mappings.transformers
- org.eclipse.persistence.mappings.xdb
- org.eclipse.persistence.oxm
- org.eclipse.persistence.oxm.annotations
- org.eclipse.persistence.oxm.attachment
- org.eclipse.persistence.oxm.documentpreservation
- org.eclipse.persistence.oxm.mappings
- org.eclipse.persistence.oxm.mappings.converters
- org.eclipse.persistence.oxm.mappings.nullpolicy
- org.eclipse.persistence.oxm.platform
- org.eclipse.persistence.oxm.record
- org.eclipse.persistence.oxm.schema
- org.eclipse.persistence.oxm.sequenced
- org.eclipse.persistence.oxm.unmapped
- org.eclipse.persistence.platform.database
- org.eclipse.persistence.platform.database.converters
- org.eclipse.persistence.platform.database.events
- org.eclipse.persistence.platform.database.jdbc
- org.eclipse.persistence.platform.database.oracle.annotations
- org.eclipse.persistence.platform.database.oracle.jdbc
- org.eclipse.persistence.platform.database.oracle.plsql
- org.eclipse.persistence.platform.database.partitioning
- org.eclipse.persistence.platform.server
- org.eclipse.persistence.platform.xml
- org.eclipse.persistence.platform.xml.jaxp
- org.eclipse.persistence.sequencing
- org.eclipse.persistence.services
- org.eclipse.persistence.services.websphere
- org.eclipse.persistence.sessions.broker
- org.eclipse.persistence.sessions.changesets
- org.eclipse.persistence.sessions.coordination
- org.eclipse.persistence.sessions.coordination.broadcast
- org.eclipse.persistence.sessions.coordination.corba
- org.eclipse.persistence.sessions.coordination.corba.sun
- org.eclipse.persistence.sessions.coordination.jms
- org.eclipse.persistence.sessions.coordination.rmi
- org.eclipse.persistence.sessions.factories
- org.eclipse.persistence.sessions.interceptors
- org.eclipse.persistence.sessions.remote
- org.eclipse.persistence.sessions.remote.corba.sun
- org.eclipse.persistence.sessions.remote.rmi
- org.eclipse.persistence.sessions.remote.rmi.iiop
- org.eclipse.persistence.sessions.serializers
- org.eclipse.persistence.sessions.server

- org.eclipse.persistence.tools
- org.eclipse.persistence.tools.file
- org.eclipse.persistence.tools.profiler
- org.eclipse.persistence.tools.schemaframework
- org.eclipse.persistence.tools.tuning
- org.eclipse.persistence.tools.weaving.jpa
- org.eclipse.persistence.transaction
- org.eclipse.persistence.transaction.was

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java Persistence API 2.1 feature:

- classloading
- jpa
- library
- transaction

## Java RESTful Services 1.1

This feature enables support for Java API for RESTful Web Services 1.1. JAX-RS annotations can be used to define web service clients and endpoints that comply with the REST architectural style. Endpoints are accessed through a common interface that is based on the HTTP standard methods.

### Enabling this feature

To enable the Java RESTful Services 1.1 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>jaxrs-1.1</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java RESTful Services 1.1 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jaxrs-1.1; type="osgi.subsystem.feature"
```

### Features that this feature enables

- json-1.0 - JavaScript Object Notation for Java
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### Standard API packages provided by this feature

- javax.ws.rs
- javax.ws.rs.core
- javax.ws.rs.ext

### IBM API packages provided by this feature

- com.ibm.websphere.jaxrs.providers.json4j
- com.ibm.websphere.jaxrs.server

### Third party API packages provided by this feature

- org.apache.wink.client
- org.apache.wink.client.handlers
- org.apache.wink.client.internal
- org.apache.wink.client.internal.handlers
- org.apache.wink.client.internal.log
- org.apache.wink.common
- org.apache.wink.common.annotations
- org.apache.wink.common.categories
- org.apache.wink.common.http
- org.apache.wink.common.internal
- org.apache.wink.common.internal.application
- org.apache.wink.common.internal.contexts
- org.apache.wink.common.internal.http
- org.apache.wink.common.internal.i18n
- org.apache.wink.common.internal.lifecycle
- org.apache.wink.common.internal.log
- org.apache.wink.common.internal.model
- org.apache.wink.common.internal.model.admin
- org.apache.wink.common.internal.properties
- org.apache.wink.common.internal.providers.entity
- org.apache.wink.common.internal.providers.entity.app
- org.apache.wink.common.internal.providers.entity.atom
- org.apache.wink.common.internal.providers.entity.csv
- org.apache.wink.common.internal.providers.entity.json
- org.apache.wink.common.internal.providers.entity.xml
- org.apache.wink.common.internal.providers.error
- org.apache.wink.common.internal.providers.header
- org.apache.wink.common.internal.providers.multipart
- org.apache.wink.common.internal.registry
- org.apache.wink.common.internal.registry.metadata
- org.apache.wink.common.internal.runtime
- org.apache.wink.common.internal.uri
- org.apache.wink.common.internal.uritemplate
- org.apache.wink.common.internal.utils
- org.apache.wink.common.model
- org.apache.wink.common.model.app
- org.apache.wink.common.model.atom
- org.apache.wink.common.model.csv
- org.apache.wink.common.model.multipart
- org.apache.wink.common.model.opensearch
- org.apache.wink.common.model.rss
- org.apache.wink.common.model.synd
- org.apache.wink.common.model.wadl
- org.apache.wink.common.utils

- org.apache.wink.jcdi.server.internal
- org.apache.wink.jcdi.server.internal.extension
- org.apache.wink.jcdi.server.internal.lifecycle
- org.apache.wink.providers.abdera
- org.apache.wink.providers.jackson
- org.apache.wink.providers.json4j
- org.apache.wink.server.handlers
- org.apache.wink.server.internal
- org.apache.wink.server.internal.application
- org.apache.wink.server.internal.contexts
- org.apache.wink.server.internal.handlers
- org.apache.wink.server.internal.handlers.ejb
- org.apache.wink.server.internal.lifecycle
- org.apache.wink.server.internal.lifecycle.metadata
- org.apache.wink.server.internal.log
- org.apache.wink.server.internal.providers.entity.html
- org.apache.wink.server.internal.providers.exception
- org.apache.wink.server.internal.registry
- org.apache.wink.server.internal.resources
- org.apache.wink.server.internal.servlet
- org.apache.wink.server.internal.servlet.contentencode
- org.apache.wink.server.internal.utils
- org.apache.wink.server.utils
- org.codehaus.jackson
- org.codehaus.jackson.annotate
- org.codehaus.jackson.impl
- org.codehaus.jackson.io
- org.codehaus.jackson.jaxrs
- org.codehaus.jackson.map
- org.codehaus.jackson.map.annotate
- org.codehaus.jackson.map.deser
- org.codehaus.jackson.map.exc
- org.codehaus.jackson.map.introspect
- org.codehaus.jackson.map.jsontype
- org.codehaus.jackson.map.jsontype.impl
- org.codehaus.jackson.map.ser
- org.codehaus.jackson.map.type
- org.codehaus.jackson.map.util
- org.codehaus.jackson.node
- org.codehaus.jackson.schema
- org.codehaus.jackson.sym
- org.codehaus.jackson.type
- org.codehaus.jackson.util
- org.codehaus.jackson.xml

## Java RESTful Services 2.0

This feature enables support for Java API for RESTful Web Services. JAX-RS annotations can be used to define web service clients and endpoints that comply with the REST architectural style. Endpoints are accessed through a common interface that is based on the HTTP standard methods.

### Enabling this feature

To enable the Java RESTful Services 2.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>jaxrs-2.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java RESTful Services 2.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jaxrs-2.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `jaxrsClient-2.0` - Java RESTful Services Client 2.0
- `json-1.0` - JavaScript Object Notation for Java
- `servlet-3.1` - Java Servlets 3.1

### Features that enable this feature

- `microProfile-1.0` - Micro Profile 1.0
- `webProfile-7.0` - Java EE Web Profile 7.0

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java RESTful Services 2.0 feature:

- `classloading`
- `library`

## Java RESTful Services Client 2.0

This feature enables support for Java Client API for JAX-RS 2.0.

### Enabling this feature

To enable the Java RESTful Services Client 2.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>jaxrsClient-2.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java RESTful Services Client 2.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jaxrsClient-2.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `json-1.0` - JavaScript Object Notation for Java
- `servlet-3.1` - Java Servlets 3.1

## Features that enable this feature

- jaxrs-2.0 - Java RESTful Services 2.0
-  zosConnect-1.2 - z/OS Connect 1.2

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java RESTful Services Client 2.0 feature:

- classloading
- library

## Java Servlets 3.0

This feature enables support for HTTP Servlets written to the Java Servlet 3.0 specification. The servlets can be packaged in Java EE specified WAR or EAR files. If servlet security is required, an `appSecurity` feature should also be configured; in the absence of a security feature any security constraints for the application will be ignored.

## Enabling this feature

To enable the Java Servlets 3.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>servlet-3.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Servlets 3.0 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.servlet-3.0; type="osgi.subsystem.feature"
```

## Features that enable this feature

- adminCenter-1.0 - Admin Center
- apiDiscovery-1.0 - API Discovery 1.0
- appSecurity-1.0 - Application Security 1.0
- batchManagement-1.0 - Batch Management
- clusterMember-1.0 - Static Cluster Member
- collectiveController-1.0 - Collective Controller
- collectiveMember-1.0 - Collective Member
- dynamicRouting-1.0 - Dynamic Routing
- healthAnalyzer-1.0 - Health Analyzer
- healthManager-1.0 - Health Manager
- httpWhiteboard-1.0 - OSGi Http Whiteboard
- jaspic-1.1 - Java Authentication SPI for Containers 1.1
- jaxrs-1.1 - Java RESTful Services 1.1
- jpa-2.0 - Java Persistence API 2.0
- jsf-2.0 - JavaServer Faces 2.0
- jsp-2.2 - JavaServer Pages 2.2
- oauth-2.0 - OAuth
- openid-2.0 - OpenID
- openidConnectClient-1.0 - OpenID Connect Client

- openidConnectServer-1.0 - OpenID Connect Provider
- osgi.jpaa-1.0 - OSGi Java Persistence API
- passwordUtilities-1.0 - Password Utilities
- restConnector-1.0 - JMX REST Connector 1.0
- restConnector-2.0 - JMX REST Connector 2.0
- rtcommGateway-1.0 - WebRTC Rtcomm Gateway
- rtcommGateway-1.0 - WebRTC Rtcomm Gateway
- samlWeb-2.0 - SAML web single sign-on version 2.0
- scalingController-1.0 - Scaling Controller
- scalingMember-1.0 - Scaling Member
- scim-1.0 - System for Cross-domain Identity Management
- sipServlet-1.1 - SIP Servlet
- spnego-1.0 - Simple and Protected GSSAPI Negotiation Mechanism
- wab-1.0 - OSGi Web Application Bundles
- webCache-1.0 - Web Response Cache
- webProfile-6.0 - Java EE Web Profile 6.0
- wsAtomicTransaction-1.2 - WS-AT Service
- wsSecuritySaml-1.1 - WSSecurity SAML
-  zosConnect-1.0 - z/OS Connect
-  zosConnect-1.2 - z/OS Connect 1.2

### Standard API packages provided by this feature

- javax.servlet
- javax.servlet.annotation
- javax.servlet.descriptor
- javax.servlet.http
- javax.servlet.resources

### IBM API packages provided by this feature

- com.ibm.websphere.servlet.container
- com.ibm.websphere.servlet.context
- com.ibm.websphere.servlet.error
- com.ibm.websphere.servlet.event
- com.ibm.websphere.servlet.session
- com.ibm.websphere.webcontainer
- com.ibm.wsspi.servlet.session

### SPI packages provided by this feature

- com.ibm.websphere.servlet.filter
- com.ibm.websphere.servlet.request
- com.ibm.websphere.servlet.response
- com.ibm.websphere.webcontainer.async
- com.ibm.ws.webcontainer.extension
- com.ibm.ws.webcontainer.spiadapter.collaborator
- com.ibm.wsspi.webcontainer
- com.ibm.wsspi.webcontainer.collaborator

- com.ibm.wsspi.webcontainer.extension
- com.ibm.wsspi.webcontainer.filter
- com.ibm.wsspi.webcontainer.metadata
- com.ibm.wsspi.webcontainer.osgi.extension
- com.ibm.wsspi.webcontainer.servlet
- com.ibm.wsspi.webcontainer.webapp

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java Servlets 3.0 feature:

- application
- applicationManager
- applicationMonitor
- channelfw
- classloading
- cors
- enterpriseApplication
- httpAccessLogging
- httpDispatcher
- httpEncoding
- httpEndpoint
- httpOptions
- httpProxyRedirect
- httpSession
- javaPermission
- library
- mimeTypeypes
- pluginConfiguration
- tcpOptions
- virtualHost
- webApplication
- webContainer

## Java Servlets 3.1

This feature enables support for HTTP Servlets written to the Java Servlet 3.1 specification. You can package servlets in Java EE specified WAR or EAR files. If servlet security is required, you should also configure an `appSecurity` feature. Without a security feature, any security constraints for the application are ignored.

### Enabling this feature

To enable the Java Servlets 3.1 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>servlet-3.1</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Servlets 3.1 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

com.ibm.websphere.appserver.servlet-3.1; type="osgi.subsystem.feature"

### Features that enable this feature

- adminCenter-1.0 - Admin Center
- apiDiscovery-1.0 - API Discovery 1.0
- appSecurity-1.0 - Application Security 1.0
- batch-1.0 - Batch API 1.0
- batchManagement-1.0 - Batch Management
- clusterMember-1.0 - Static Cluster Member
- collectiveController-1.0 - Collective Controller
- collectiveMember-1.0 - Collective Member
- dynamicRouting-1.0 - Dynamic Routing
- healthAnalyzer-1.0 - Health Analyzer
- healthManager-1.0 - Health Manager
- httpWhiteboard-1.0 - OSGi Http Whiteboard
- jaspic-1.1 - Java Authentication SPI for Containers 1.1
- javaee-7.0 - Java EE Full Platform 7.0
- jaxrs-1.1 - Java RESTful Services 1.1
- jaxrs-2.0 - Java RESTful Services 2.0
- jaxrsClient-2.0 - Java RESTful Services Client 2.0
- jpa-2.0 - Java Persistence API 2.0
- jsf-2.0 - JavaServer Faces 2.0
- jsf-2.2 - JavaServer Faces 2.2
- jsp-2.2 - JavaServer Pages 2.2
- jsp-2.3 - JavaServer Pages 2.3
- oauth-2.0 - OAuth
- openid-2.0 - OpenID
- openidConnectClient-1.0 - OpenID Connect Client
- openidConnectServer-1.0 - OpenID Connect Provider
- osgi.jpa-1.0 - OSGi Java Persistence API
- passwordUtilities-1.0 - Password Utilities
- restConnector-1.0 - JMX REST Connector 1.0
- restConnector-2.0 - JMX REST Connector 2.0
- rtcomm-1.0 - Real-Time Communications
- rtcommGateway-1.0 - WebRTC Rtcomm Gateway
- samlWeb-2.0 - SAML web single sign-on version 2.0
- scalingController-1.0 - Scaling Controller
- scalingMember-1.0 - Scaling Member
- scim-1.0 - System for Cross-domain Identity Management
- sipServlet-1.1 - SIP Servlet
- spnego-1.0 - Simple and Protected GSSAPI Negotiation Mechanism
- wab-1.0 - OSGi Web Application Bundles
- webCache-1.0 - Web Response Cache
- webProfile-7.0 - Java EE Web Profile 7.0
- websocket-1.0 - Java WebSocket 1.0

- websocket-1.1 - Java WebSocket 1.1
- wsAtomicTransaction-1.2 - WS-AT Service
- wsSecuritySaml-1.1 - WSSecurity SAML
-  zosConnect-1.0 - z/OS Connect
-  zosConnect-1.2 - z/OS Connect 1.2

### Standard API packages provided by this feature

- javax.servlet
- javax.servlet.annotation
- javax.servlet.descriptor
- javax.servlet.http
- javax.servlet.resources

### IBM API packages provided by this feature

- com.ibm.websphere.servlet.container
- com.ibm.websphere.servlet.context
- com.ibm.websphere.servlet.error
- com.ibm.websphere.servlet.event
- com.ibm.websphere.servlet.session
- com.ibm.websphere.webcontainer
- com.ibm.wsspi.servlet.session

### SPI packages provided by this feature

- com.ibm.websphere.servlet.filter
- com.ibm.websphere.servlet.request
- com.ibm.websphere.servlet.response
- com.ibm.websphere.webcontainer.async
- com.ibm.ws.webcontainer.extension
- com.ibm.ws.webcontainer.spiadapter.collaborator
- com.ibm.wsspi.webcontainer
- com.ibm.wsspi.webcontainer.collaborator
- com.ibm.wsspi.webcontainer.extension
- com.ibm.wsspi.webcontainer.filter
- com.ibm.wsspi.webcontainer.metadata
- com.ibm.wsspi.webcontainer.osgi.extension
- com.ibm.wsspi.webcontainer.servlet
- com.ibm.wsspi.webcontainer.webapp

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java Servlets 3.1 feature:

- application
- applicationManager
- applicationMonitor
- channelfw
- classloading

- cors
- enterpriseApplication
- httpAccessLogging
- httpDispatcher
- httpEncoding
- httpEndpoint
- httpOptions
- httpProxyRedirect
- httpSession
- javaPermission
- library
- mimeTypeypes
- pluginConfiguration
- tcpOptions
- virtualHost
- webApplication
- webContainer

## Java Web Services 2.2

This feature enables support for Java API for XML-Based Web Services 2.2. JAX-WS web services and clients communicate using XML. Annotations can be used to simplify the development of JAX-WS clients and endpoints.

### Enabling this feature

To enable the Java Web Services 2.2 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jaxws-2.2</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java Web Services 2.2 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jaxws-2.2; type="osgi.subsystem.feature"
```

### Features that this feature enables

- jaxb-2.2 - Java XML Bindings 2.2

### Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0
- wsAtomicTransaction-1.2 - WS-AT Service
- wsSecurity-1.1 - Web Service Security

### Standard API packages provided by this feature

- javax.wsdl
- javax.wsdl.extensions
- javax.wsdl.extensions.http
- javax.wsdl.extensions.mime
- javax.wsdl.extensions.schema

- javax.wsdl.extensions.soap
- javax.wsdl.extensions.soap12
- javax.wsdl.factory
- javax.wsdl.xml
- javax.xml.ws
- javax.xml.ws.handler
- javax.xml.ws.handler.soap
- javax.xml.ws.http
- javax.xml.ws.soap
- javax.xml.ws.spi
- javax.xml.ws.spi.http
- javax.xml.ws.wsaddressing

### **SPI packages provided by this feature**

- com.ibm.wsspi.webservices.handler

### **Feature configuration elements**

You can use the following elements in your `server.xml` file to configure the Java Web Services 2.2 feature:

- classloading
- library

### **Java WebSocket 1.0**

This feature enables support for WebSocket applications written to the Java API for WebSocket 1.0 specification.

### **Enabling this feature**

To enable the Java WebSocket 1.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>websocket-1.0</feature>
```

### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the Java WebSocket 1.0 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.websocket-1.0; type="osgi.subsystem.feature"
```

### **Features that this feature enables**

- servlet-3.1 - Java Servlets 3.1

### **Standard API packages provided by this feature**

- javax.websocket
- javax.websocket.server

### **IBM API packages provided by this feature**

- com.ibm.websphere.wsoc

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java WebSocket 1.0 feature:

- `wsocOutbound`

## Java WebSocket 1.1

This feature enables support for WebSocket applications written to the Java API for WebSocket 1.1 specification.

### Enabling this feature

To enable the Java WebSocket 1.1 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>websocket-1.1</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java WebSocket 1.1 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.websocket-1.1; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `servlet-3.1` - Java Servlets 3.1

### Features that enable this feature

- `webProfile-7.0` - Java EE Web Profile 7.0

### Standard API packages provided by this feature

- `javax.websocket`
- `javax.websocket.server`

### IBM API packages provided by this feature

- `com.ibm.websphere.wsoc`

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java WebSocket 1.1 feature:

- `wsocOutbound`

## Java XML Bindings 2.2

This feature enables support for the Java Architecture for XML Binding 2.2 specification, which provides easy mapping of Java classes to XML documents.

### Enabling this feature

To enable the Java XML Bindings 2.2 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>jaxb-2.2</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Java XML Bindings 2.2 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jaxb-2.2; type="osgi.subsystem.feature"
```

### Features that enable this feature

- javaeeClient-7.0 - Java EE V7 Application Client
- jaxws-2.2 - Java Web Services 2.2

### Standard API packages provided by this feature

- javax.xml.bind
- javax.xml.bind.annotation
- javax.xml.bind.annotation.adapters
- javax.xml.bind.attachment
- javax.xml.bind.helpers
- javax.xml.bind.util

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Java XML Bindings 2.2 feature:

- classloading
- library

### JavaMail 1.5

This feature allows applications to utilize the JavaMail 1.5 API.

### Enabling this feature

To enable the JavaMail 1.5 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>javaMail-1.5</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the JavaMail 1.5 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.javaMail-1.5; type="osgi.subsystem.feature"
```

### Features that enable this feature

- javaee-7.0 - Java EE Full Platform 7.0
- javaeeClient-7.0 - Java EE V7 Application Client

### Standard API packages provided by this feature

- javax.mail
- javax.mail.event
- javax.mail.internet
- javax.mail.search
- javax.mail.util

### Third party API packages provided by this feature

- com.sun.mail
- com.sun.mail.auth
- com.sun.mail.handlers
- com.sun.mail.iap
- com.sun.mail.imap
- com.sun.mail.imap.protocol
- com.sun.mail.pop3
- com.sun.mail.smtp
- com.sun.mail.util
- com.sun.mail.util.logging

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the JavaMail 1.5 feature:

- mailSession

### JavaScript Object Notation Processing

The Java API for JSON Processing (JSON-P) feature provides a standardized method for constructing and manipulating data to be rendered in JavaScript Object Notation (JSON).

### Enabling this feature

To enable the JavaScript Object Notation Processing feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>jsonp-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the JavaScript Object Notation Processing feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jsonp-1.0; type="osgi.subsystem.feature"
```

### Features that enable this feature

- javaeeClient-7.0 - Java EE V7 Application Client
- microProfile-1.0 - Micro Profile 1.0
- webProfile-7.0 - Java EE Web Profile 7.0

### Standard API packages provided by this feature

- javax.json
- javax.json.spi
- javax.json.stream

### JavaScript Object Notation for Java

This feature provides access to the JavaScript Object Notation (JSON4J) library. The JSON4J library provides a simple Java model for constructing and manipulating data to be rendered as JSON data.

## Enabling this feature

To enable the JavaScript Object Notation for Java feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>json-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the JavaScript Object Notation for Java feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.json-1.0; type="osgi.subsystem.feature"
```

## Features that enable this feature

- adminCenter-1.0 - Admin Center
- apiDiscovery-1.0 - API Discovery 1.0
- batchManagement-1.0 - Batch Management
- collectiveController-1.0 - Collective Controller
- dynamicRouting-1.0 - Dynamic Routing
- healthAnalyzer-1.0 - Health Analyzer
- healthManager-1.0 - Health Manager
- jaxrs-1.1 - Java RESTful Services 1.1
- jaxrs-2.0 - Java RESTful Services 2.0
- jaxrsClient-2.0 - Java RESTful Services Client 2.0
- oauth-2.0 - OAuth
- restConnector-1.0 - JMX REST Connector 1.0
- restConnector-2.0 - JMX REST Connector 2.0
- rtcomm-1.0 - Real-Time Communications
- scalingController-1.0 - Scaling Controller
- scalingMember-1.0 - Scaling Member
- scim-1.0 - System for Cross-domain Identity Management
-  zosConnect-1.0 - z/OS Connect
-  zosConnect-1.2 - z/OS Connect 1.2

## IBM API packages provided by this feature

- com.ibm.json.java
- com.ibm.json.xml

## JavaServer Faces 2.0

This feature enables support for web applications that use the Java Server Faces (JSF) framework. This framework simplifies the construction of user interfaces.

## Enabling this feature

To enable the JavaServer Faces 2.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jsf-2.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the JavaServer Faces 2.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jsf-2.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- beanValidation-1.0 - Bean Validation 1.0
- beanValidation-1.1 - Bean Validation 1.1
- jsp-2.2 - JavaServer Pages 2.2
- jsp-2.3 - JavaServer Pages 2.3
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

## Features that enable this feature

- webProfile-6.0 - Java EE Web Profile 6.0

## Standard API packages provided by this feature

- javax.faces
- javax.faces.application
- javax.faces.bean
- javax.faces.component
- javax.faces.component.behavior
- javax.faces.component.html
- javax.faces.component.visit
- javax.faces.context
- javax.faces.convert
- javax.faces.el
- javax.faces.event
- javax.faces.lifecycle
- javax.faces.model
- javax.faces.render
- javax.faces.validator
- javax.faces.view
- javax.faces.view.facelets
- javax.faces.webapp
- javax.persistence

## Feature configuration elements

You can use the following elements in your server.xml file to configure the JavaServer Faces 2.0 feature:

- classloading
- transaction

## JavaServer Faces 2.2

This feature enables support for web applications that use the Java Server Faces (JSF) 2.2 framework. This framework simplifies the construction of user interfaces.

### Enabling this feature

To enable the JavaServer Faces 2.2 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>jsf-2.2</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the JavaServer Faces 2.2 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jsf-2.2; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `jsp-2.3` - JavaServer Pages 2.3
- `servlet-3.1` - Java Servlets 3.1

### Features that enable this feature

- `webProfile-7.0` - Java EE Web Profile 7.0

### Standard API packages provided by this feature

- `javax.faces`
- `javax.faces.application`
- `javax.faces.bean`
- `javax.faces.component`
- `javax.faces.component.behavior`
- `javax.faces.component.html`
- `javax.faces.component.visit`
- `javax.faces.context`
- `javax.faces.convert`
- `javax.faces.el`
- `javax.faces.event`
- `javax.faces.flow`
- `javax.faces.flow.builder`
- `javax.faces.lifecycle`
- `javax.faces.model`
- `javax.faces.render`
- `javax.faces.validator`
- `javax.faces.view`
- `javax.faces.view.facelets`
- `javax.faces.webapp`

## JavaServer Pages 2.2

This feature enables support for Java Server Pages (JSPs) that are written to the JSP 2.2 specification. This framework simplifies the construction of user interfaces.

## Enabling this feature

To enable the JavaServer Pages 2.2 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jsp-2.2</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the JavaServer Pages 2.2 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jsp-2.2; type="osgi.subsystem.feature"
```

## Features that this feature enables

- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

## Features that enable this feature

- adminCenter-1.0 - Admin Center
- jsf-2.0 - JavaServer Faces 2.0
- oauth-2.0 - OAuth
- openidConnectClient-1.0 - OpenID Connect Client
- openidConnectServer-1.0 - OpenID Connect Provider
- webCache-1.0 - Web Response Cache
- webProfile-6.0 - Java EE Web Profile 6.0

## Standard API packages provided by this feature

- javax.el
- javax.servlet.jsp
- javax.servlet.jsp.el
- javax.servlet.jsp.jstl.core
- javax.servlet.jsp.jstl.fmt
- javax.servlet.jsp.jstl.sql
- javax.servlet.jsp.jstl.tlv
- javax.servlet.jsp.resources
- javax.servlet.jsp.tagext

## SPI packages provided by this feature

- com.ibm.wsspi.jsp.taglib.config

## Feature configuration elements

You can use the following elements in your server.xml file to configure the JavaServer Pages 2.2 feature:

- jspEngine

## JavaServer Pages 2.3

This feature enables support for Java Server Pages (JSPs) that are written to the JSP 2.3 specification. This framework simplifies the construction of user interfaces. Enabling this feature also enables the Expression Language (EL) version 3.0 feature.

## Enabling this feature

To enable the JavaServer Pages 2.3 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>jsp-2.3</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the JavaServer Pages 2.3 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.jsp-2.3; type="osgi.subsystem.feature"
```

## Features that this feature enables

- el-3.0 - Expression Language 3.0
- servlet-3.1 - Java Servlets 3.1

## Features that enable this feature

- adminCenter-1.0 - Admin Center
- jsf-2.0 - JavaServer Faces 2.0
- jsf-2.2 - JavaServer Faces 2.2
- oauth-2.0 - OAuth
- openidConnectClient-1.0 - OpenID Connect Client
- openidConnectServer-1.0 - OpenID Connect Provider
- webCache-1.0 - Web Response Cache
- webProfile-7.0 - Java EE Web Profile 7.0

## Standard API packages provided by this feature

- javax.el
- javax.servlet.jsp
- javax.servlet.jsp.el
- javax.servlet.jsp.jstl.core
- javax.servlet.jsp.jstl.fmt
- javax.servlet.jsp.jstl.sql
- javax.servlet.jsp.jstl.tlv
- javax.servlet.jsp.tagext

## SPI packages provided by this feature

- com.ibm.wsspi.jsp.taglib.config

## Feature configuration elements

You can use the following elements in your server.xml file to configure the JavaServer Pages 2.3 feature:

- jspEngine

## Job Manager Integration

This feature enables Liberty profile servers to automatically publish their status to the WebSphere Application Server Job Managers. This feature is required for the Job Manager to discover server instances that it did not start.

## Enabling this feature

To enable the Job Manager Integration feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>serverStatus-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Job Manager Integration feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.serverStatus-1.0; type="osgi.subsystem.feature"
```

## LDAP User Registry

This feature enables support for using an LDAP server as a user registry. Any server that supports LDAP Version 3.0 may be used. Multiple LDAP registries can be configured, and then federated to achieve a single logical registry view.

## Enabling this feature

To enable the LDAP User Registry feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>ldapRegistry-3.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the LDAP User Registry feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.ldapRegistry-3.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- federatedRegistry-1.0 - Federated User Registry

## Features that enable this feature

- appSecurity-1.0 - Application Security 1.0
- oauth-2.0 - OAuth

## Feature configuration elements

You can use the following elements in your server.xml file to configure the LDAP User Registry feature:

- activeLdapFilterProperties
- administrator-role
- classloading

- customLdapFilterProperties
- domino50LdapFilterProperties
- edirectoryLdapFilterProperties
- idsLdapFilterProperties
- iplanetLdapFilterProperties
- ldapRegistry
- library
- netscapeLdapFilterProperties
- securewayLdapFilterProperties

## Logstash Collector 1.0

Logstash collector gathers data from various sources and forwards the data to a Logstash server using Lumberjack protocol.

### Enabling this feature

To enable the Logstash Collector 1.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>logstashCollector-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Logstash Collector 1.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.logstashCollector-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- ssl-1.0 - Secure Socket Layer

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Logstash Collector 1.0 feature:

- channelfw
- classloading
- httpAccessLogging
- httpDispatcher
- httpEncoding
- httpEndpoint
- httpOptions
- httpProxyRedirect
- logstashCollector
- mimeTypeypes
- tcpOptions
- virtualHost

## Media Server Control

The Liberty Media Server Control feature (mediaServerControl-1.0) enables the ability to access media servers via the JSR309 API. For applications to use this API, a driver implementation of JSR309 must be installed.

### Enabling this feature

To enable the Media Server Control feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>mediaServerControl-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Media Server Control feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.mediaServerControl-1.0; type="osgi.subsystem.feature"
```

### Standard API packages provided by this feature

- javax.media.mscontrol
- javax.media.mscontrol.join
- javax.media.mscontrol.mediagroup
- javax.media.mscontrol.mediagroup.http
- javax.media.mscontrol.mediagroup.rtp
- javax.media.mscontrol.mediagroup.signals
- javax.media.mscontrol.mixer
- javax.media.mscontrol.networkconnection
- javax.media.mscontrol.resource
- javax.media.mscontrol.resource.common
- javax.media.mscontrol.resource.enums
- javax.media.mscontrol.resource.video
- javax.media.mscontrol.spi
- javax.media.mscontrol.vxml

## Message Server 1.0

This feature enables an embedded messaging server that is JMS compliant. Applications can send and receive messages using the wasJmsClient feature.

### Enabling this feature

To enable the Message Server 1.0 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>wasJmsServer-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7

- JavaSE-1.8

### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the Message Server 1.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.wasJmsServer-1.0; type="osgi.subsystem.feature"
```

### **Features that enable this feature**

- javaee-7.0 - Java EE Full Platform 7.0

### **IBM API packages provided by this feature**

- com.ibm.websphere.messaging.mbean

### **Feature configuration elements**

You can use the following elements in your `server.xml` file to configure the Message Server 1.0 feature:

- channelfw
- classloading
- messagingEngine
- tcpOptions
- transaction
- wasJmsEndpoint
- wasJmsOutbound

### **Message Server Security 1.0**

This feature enables the WebSphere Embedded Messaging Server to authenticate and authorize access from JMS clients.

### **Enabling this feature**

To enable the Message Server Security 1.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>wasJmsSecurity-1.0</feature>
```

### **Supported Java Versions**

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the Message Server Security 1.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.wasJmsSecurity-1.0; type="osgi.subsystem.feature"
```

### **Features that this feature enables**

- ssl-1.0 - Secure Socket Layer

### **Features that enable this feature**

- javaee-7.0 - Java EE Full Platform 7.0

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Message Server Security 1.0 feature:

- administrator-role
- authCache
- authentication
- basicRegistry
- classloading
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- quickStartSecurity

## Message-Driven Beans 3.1

This feature enables the use of Message-Driven Enterprise JavaBeans. MDBs allow asynchronous processing of messages within a Java EE component.

### Enabling this feature

To enable the Message-Driven Beans 3.1 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>mdb-3.1</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Message-Driven Beans 3.1 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.mdb-3.1; type="osgi.subsystem.feature"
```

### Features that this feature enables

- jca-1.6 - Java Connector Architecture 1.6
- jndi-1.0 - Java Naming and Directory Interface

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Message-Driven Beans 3.1 feature:

- application
- applicationManager
- applicationMonitor
- classloading
- ejbApplication
- ejbContainer

- enterpriseApplication
- javaPermission
- library
- transaction
- webApplication

## Message-Driven Beans 3.2

This feature enables the use of Message-Driven Enterprise JavaBeans written to the EJB 3.2 specification. MDBs allow asynchronous processing of messages within a Java EE component.

### Enabling this feature

To enable the Message-Driven Beans 3.2 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>mdb-3.2</feature>
```

### Supported Java Versions

- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Message-Driven Beans 3.2 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.mdb-3.2; type="osgi.subsystem.feature"
```

### Features that this feature enables

- jca-1.7 - Java Connector Architecture 1.7
- jndi-1.0 - Java Naming and Directory Interface

### Features that enable this feature

- ejb-3.2 - Enterprise JavaBeans 3.2
- jmsMdb-3.2 - JMS Message-Driven Beans 3.2

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Message-Driven Beans 3.2 feature:

- application
- applicationManager
- applicationMonitor
- classloading
- ejbApplication
- ejbContainer
- enterpriseApplication
- javaPermission
- library
- transaction
- webApplication

## Micro Profile 1.0

This feature combines the Liberty features that support the Micro Profile for enterprise Java.

### Enabling this feature

To enable the Micro Profile 1.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>microProfile-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Micro Profile 1.0 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.microProfile-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- cdi-1.2 - Contexts and Dependency Injection 1.2
- jaxrs-2.0 - Java RESTful Services 2.0
- jsonp-1.0 - JavaScript Object Notation Processing

## MongoDB Integration 2.0

This feature enables the usage of the MongoDB Java Driver and allows DB instances to be configured in the server configuration, injected into managed components such as EJBs, and accessed through JNDI. Applications interact with these DB instances via the MongoDB APIs

### Enabling this feature

To enable the MongoDB Integration 2.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>mongodb-2.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the MongoDB Integration 2.0 feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.mongodb-2.0; type="osgi.subsystem.feature"
```

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the MongoDB Integration 2.0 feature:

- classloading
- library
- mongo
- mongoDB

## OAuth

This feature enables web applications to integrate OAuth 2.0 for authenticating and authorizing users.

## Enabling this feature

To enable the OAuth feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>oauth-2.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the OAuth feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.oauth-2.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- `appSecurity-2.0` - Application Security 2.0
- `distributedMap-1.0` - Distributed Map interface for Dynamic Caching
- `json-1.0` - JavaScript Object Notation for Java
- `jsp-2.2` - JavaServer Pages 2.2
- `jsp-2.3` - JavaServer Pages 2.3
- `ldapRegistry-3.0` - LDAP User Registry
- `servlet-3.0` - Java Servlets 3.0
- `servlet-3.1` - Java Servlets 3.1
- `ssl-1.0` - Secure Socket Layer

## Features that enable this feature

- `openidConnectClient-1.0` - OpenID Connect Client
- `openidConnectServer-1.0` - OpenID Connect Provider

## IBM API packages provided by this feature

- `com.ibm.oauth.core.api.attributes`
- `com.ibm.oauth.core.api.config`
- `com.ibm.oauth.core.api.error`
- `com.ibm.oauth.core.api.error.oauth20`
- `com.ibm.oauth.core.api.oauth20.mediator`
- `com.ibm.websphere.security.oauth20`
- `com.ibm.websphere.security.openidconnect.token`
- `com.ibm.wsspi.security.oauth20.token`

## SPI packages provided by this feature

- `com.ibm.wsspi.security.oauth20`
- `com.ibm.wsspi.security.openidconnect`

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the OAuth feature:

- `administrator-role`
- `authCache`
- `authentication`
- `authorization-roles`
- `basicRegistry`

- classloading
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- oauth-roles
- oauthProvider
- quickStartSecurity
- trustAssociation

## OSGi Application Integration

This feature adds local application-to-application integration for OSGi Applications.

### Enabling this feature

To enable the OSGi Application Integration feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>osgiAppIntegration-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the OSGi Application Integration feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.ws.eba.app.integration-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- blueprint-1.0 - OSGi Blueprint

### Feature configuration elements

You can use the following elements in your server.xml file to configure the OSGi Application Integration feature:

- classloading
- transaction

## OSGi Blueprint

This feature enables support for deploying OSGi applications that use the OSGi blueprint container specification. With the OSGi Applications support in WebSphere Application Server, you can develop and deploy modular applications that use Java EE and OSGi technologies.

### Enabling this feature

To enable the OSGi Blueprint feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>blueprint-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the OSGi Blueprint feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.blueprint-1.0; type="osgi.subsystem.feature"
```

## Features that enable this feature

- osgi.jpa-1.0 - OSGi Java Persistence API
- osgiAppIntegration-1.0 - OSGi Application Integration
- wab-1.0 - OSGi Web Application Bundles

## Standard API packages provided by this feature

- org.apache.aries.blueprint
- org.apache.aries.blueprint.ext
- org.apache.aries.blueprint.ext.evaluator
- org.apache.aries.blueprint.mutable
- org.apache.aries.blueprint.services
- org.apache.aries.blueprint.utils
- org.apache.aries.util
- org.osgi.framework
- org.osgi.framework.hooks.bundle
- org.osgi.framework.hooks.resolver
- org.osgi.framework.hooks.service
- org.osgi.framework.hooks.weaving
- org.osgi.framework.launch
- org.osgi.framework.namespace
- org.osgi.framework.startlevel
- org.osgi.framework.wiring
- org.osgi.resource
- org.osgi.service.blueprint
- org.osgi.service.blueprint.container
- org.osgi.service.blueprint.reflect
- org.osgi.service.component
- org.osgi.service.condpermadmin
- org.osgi.service.jndi
- org.osgi.service.packageadmin
- org.osgi.service.startlevel
- org.osgi.service.url
- org.osgi.util.tracker

## Third party API packages provided by this feature

- org.apache.aries.transaction.exception

## SPI packages provided by this feature

- org.apache.aries.blueprint
- org.apache.aries.blueprint.ext
- org.apache.aries.blueprint.ext.evaluator
- org.apache.aries.blueprint.mutable
- org.apache.aries.blueprint.services
- org.apache.aries.util
- org.osgi.service.cm
- org.osgi.service.subsystem

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the OSGi Blueprint feature:

- application
- applicationManager
- applicationMonitor
- bundleRepository
- classloading
- javaPermission
- library
- osgiApplication
- osgiApplications
- osgiLibrary
- transaction

## OSGi Bundle

This feature enables support for deploying OSGi applications. With the OSGi Applications support in WebSphere Application Server, you can develop and deploy modular applications that use Java EE and OSGi technologies.

## Enabling this feature

To enable the OSGi Bundle feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>osgiBundle-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the OSGi Bundle feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.osgiBundle-1.0; type="osgi.subsystem.feature"
```

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the OSGi Bundle feature:

- `application`
- `applicationManager`
- `applicationMonitor`
- `bundleRepository`
- `classloading`
- `javaPermission`
- `library`
- `osgiApplication`
- `osgiApplications`
- `osgiLibrary`

## OSGi Debug Console

This feature enables an OSGi console to aid debug of the runtime. It can be used to display information about bundles, packages and services which may be useful when developing your own features for product extensions.

### Enabling this feature

To enable the OSGi Debug Console feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>osgiConsole-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the OSGi Debug Console feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.osgiConsole-1.0; type="osgi.subsystem.feature"
```

## OSGi Http Whiteboard

This feature enables deploying modular Web applications written using Servlet technologies and the OSGi HTTP Whiteboard specification.

### Enabling this feature

To enable the OSGi Http Whiteboard feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>httpWhiteboard-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the OSGi Http Whiteboard feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.httpWhiteboard-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `servlet-3.0` - Java Servlets 3.0
- `servlet-3.1` - Java Servlets 3.1

## Standard API packages provided by this feature

- org.osgi.service.http
- org.osgi.service.http.context
- org.osgi.service.http.whiteboard

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the OSGi Http Whiteboard feature:

- channelfw
- classloading
- httpAccessLogging
- httpDispatcher
- httpEncoding
- httpEndpoint
- httpOptions
- httpProxyRedirect
- httpWhiteboard
- mimeTypeypes
- tcpOptions
- virtualHost

## OSGi Java Persistence API

This feature is superseded by the `blueprint-1.0` and `jpa-2.0` features. When those features are both added to the server, this feature is added automatically.

## Enabling this feature

To enable the OSGi Java Persistence API feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>osgi.jpa-1.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the OSGi Java Persistence API feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.osgi.jpa-1.0; type="osgi.subsystem.feature"
```

## Features that this feature is superseded by

- `blueprint-1.0` - OSGi Blueprint
- `jpa-2.0` - Java Persistence API 2.0

## Features that this feature enables

- `beanValidation-1.0` - Bean Validation 1.0
- `beanValidation-1.1` - Bean Validation 1.1
- `blueprint-1.0` - OSGi Blueprint
- `jdbc-4.0` - Java Database Connectivity 4.0
- `jdbc-4.1` - Java Database Connectivity 4.1
- `jndi-1.0` - Java Naming and Directory Interface
- `jpa-2.0` - Java Persistence API 2.0

- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the OSGi Java Persistence API feature:

- classloading
- transaction

### OSGi Web Application Bundles

This feature enables OSGi applications that contain Web Application Bundles (WABs). Web application bundles are OSGi bundles that are internally structured in the same way as a war file and support the same web components.

### Enabling this feature

To enable the OSGi Web Application Bundles feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>wab-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the OSGi Web Application Bundles feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.wab-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- blueprint-1.0 - OSGi Blueprint
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### Features that enable this feature

- wsAtomicTransaction-1.2 - WS-AT Service

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the OSGi Web Application Bundles feature:

- classloading
- transaction

### OpenID

This feature enables web applications to integrate OpenID 2.0 for authenticating users instead of, or in addition to, the configured user registry.

### Enabling this feature

To enable the OpenID feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>openid-2.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the OpenID feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.openid-2.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- appSecurity-2.0 - Application Security 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the OpenID feature:

- `authFilter`
- `openId`
- `userInfo`

## OpenID Connect Client

This feature enables web applications to integrate OpenID Connect Client 1.0 for authenticating users instead of, or in addition to, the configured user registry.

### Enabling this feature

To enable the OpenID Connect Client feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>openidConnectClient-1.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the OpenID Connect Client feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.openidConnectClient-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- distributedMap-1.0 - Distributed Map interface for Dynamic Caching
- jsp-2.2 - JavaServer Pages 2.2
- jsp-2.3 - JavaServer Pages 2.3
- oauth-2.0 - OAuth
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1
- ssl-1.0 - Secure Socket Layer

### IBM API packages provided by this feature

- `com.ibm.websphere.security.openidconnect`

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the OpenID Connect Client feature:

- `administrator-role`
- `authCache`

- authFilter
- authentication
- authorization-roles
- basicRegistry
- classloading
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- openidConnectClient
- quickStartSecurity
- trustAssociation

## OpenID Connect Provider

This feature enables web applications to integrate OpenID Connect Server 1.0 for authenticating users instead of, or in addition to, the configured user registry.

### Enabling this feature

To enable the OpenID Connect Provider feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>openidConnectServer-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the OpenID Connect Provider feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.openidConnectServer-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- jsp-2.2 - JavaServer Pages 2.2
- jsp-2.3 - JavaServer Pages 2.3
- oauth-2.0 - OAuth
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### IBM API packages provided by this feature

- com.ibm.websphere.security.openidconnect

### Feature configuration elements

You can use the following elements in your server.xml file to configure the OpenID Connect Provider feature:

- openidConnectProvider

### Password Utilities

This feature enables support for obtaining the values of the user and password attributes of authData elements from an application, and also allows the use of the com.ibm.websphere.crypto.PasswordUtil class as an API.

## Enabling this feature

To enable the Password Utilities feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>passwordUtilities-1.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Password Utilities feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.passwordUtilities-1.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- appSecurity-1.0 - Application Security 1.0
- appSecurity-2.0 - Application Security 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

## IBM API packages provided by this feature

- com.ibm.websphere.crypto
- com.ibm.websphere.security.auth.data
- com.ibm.websphere.security.jca

## Feature configuration elements

You can use the following elements in your server.xml file to configure the Password Utilities feature:

- authData
- classloading
- jaasLoginContextEntry
- jaasLoginModule
- transaction

## Performance Monitoring

This feature enables the Performance Monitoring Infrastructure (PMI) for other features the server is running. Monitoring data is accessible through standard MXBeans; access through the traditional WebSphere Perf MBean can be enabled.

## Enabling this feature

To enable the Performance Monitoring feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>monitor-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Performance Monitoring feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.monitor-1.0; type="osgi.subsystem.feature"
```

## IBM API packages provided by this feature

- `com.ibm.websphere.monitor.jmx`

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Performance Monitoring feature:

- `classloading`
- `monitor`

## Real-Time Communications

The Liberty Real-Time Communications feature (`rtcomm-1.0`) enables a highly-scalable signaling infrastructure that can be used to connect WebRTC clients and other types of IoT nodes into real-time audio/video/data interactions.

## Enabling this feature

To enable the Real-Time Communications feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>rtcomm-1.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Real-Time Communications feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.rtcomm-1.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- `json-1.0` - JavaScript Object Notation for Java
- `servlet-3.1` - Java Servlets 3.1

## Features that enable this feature

- `rtcommGateway-1.0` - WebRTC Rtcomm Gateway

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Real-Time Communications feature:

- `rtcomm`

## Request Timing

Provides warnings and diagnostic info for slow or hung requests.

## Enabling this feature

To enable the Request Timing feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>requestTiming-1.0</feature>
```

## Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Request Timing feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.requestTiming-1.0; type="osgi.subsystem.feature"
```

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Request Timing feature:

- `requestTiming`

## SAML web single sign-on version 2.0

This feature enables web applications to use SAML web single sign-on version 2.0 function.

## Enabling this feature

To enable the SAML web single sign-on version 2.0 feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>samlWeb-2.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the SAML web single sign-on version 2.0 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.samlWeb-2.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- `appSecurity-2.0` - Application Security 2.0
- `distributedMap-1.0` - Distributed Map interface for Dynamic Caching
- `servlet-3.0` - Java Servlets 3.0
- `servlet-3.1` - Java Servlets 3.1
- `ssl-1.0` - Secure Socket Layer

## Features that enable this feature

- `wsSecuritySaml-1.1` - WSSecurity SAML

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the SAML web single sign-on version 2.0 feature:

- `administrator-role`
- `authCache`
- `authFilter`
- `authentication`
- `authorization-roles`
- `basicRegistry`

- classloading
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- quickStartSecurity
- samlWebSso20
- trustAssociation

## SIP Servlet

This feature enables support for SIP Servlets written to the Java SipServlet 1.1 specification. The servlets can be packaged in Java EE specified WAR, SAR or EAR files. If servlet security is required, an appSecurity feature should also be configured; in the absence of a security feature any security constraints for the application will be ignored.

### Enabling this feature

To enable the SIP Servlet feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>sipServlet-1.1</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the SIP Servlet feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.sipServlet-1.1; type="osgi.subsystem.feature"
```

### Features that this feature enables

- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### Features that enable this feature

- rtcommGateway-1.0 - WebRTC Rtcomm Gateway

### Standard API packages provided by this feature

- javax.servlet.sip
- javax.servlet.sip.annotation
- javax.servlet.sip.ar
- javax.servlet.sip.ar.spi

### IBM API packages provided by this feature

- com.ibm.websphere.sip
- com.ibm.websphere.sip.resolver
- com.ibm.websphere.sip.resolver.events
- com.ibm.websphere.sip.resolver.exception
- com.ibm.websphere.sip.unmatchedMessages
- com.ibm.websphere.sip.unmatchedMessages.events

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the SIP Servlet feature:

- `channelfw`
- `domainResolver`
- `sipApplicationRouter`
- `sipContainer`
- `sipEndpoint`
- `sipStack`
- `tcpOptions`

## Scaling Controller

The Scaling Controller feature manages Liberty clusters by starting and stopping servers based on Scaling Policy.

### Enabling this feature

To enable the Scaling Controller feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>scalingController-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Scaling Controller feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.scalingController-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `collectiveController-1.0` - Collective Controller
- `json-1.0` - JavaScript Object Notation for Java
- `restConnector-1.0` - JMX REST Connector 1.0
- `restConnector-2.0` - JMX REST Connector 2.0
- `servlet-3.0` - Java Servlets 3.0
- `servlet-3.1` - Java Servlets 3.1

### IBM API packages provided by this feature

- `com.ibm.websphere.scaling.manager.stack`

### SPI packages provided by this feature

- `com.ibm.wsspi.scaling.action.consumer`
- `com.ibm.wsspi.scaling.action.controller`

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Scaling Controller feature:

- `installable`
- `package`
- `scalingDefinitions`
- `stackGroup`
- `stackManager`

## Scaling Member

The Scaling Member feature allows a Liberty clustered server to be managed by a Liberty Scaling Controller server. The Scaling Controller directs the Scaling Member to start and stop based on Scaling Controller policies.

### Enabling this feature

To enable the Scaling Member feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>scalingMember-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Scaling Member feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.scalingMember-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `clusterMember-1.0` - Static Cluster Member
- `collectiveMember-1.0` - Collective Member
- `json-1.0` - JavaScript Object Notation for Java
- `restConnector-1.0` - JMX REST Connector 1.0
- `restConnector-2.0` - JMX REST Connector 2.0
- `servlet-3.0` - Java Servlets 3.0
- `servlet-3.1` - Java Servlets 3.1

### IBM API packages provided by this feature

- `com.ibm.websphere.scaling.member`

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Scaling Member feature:

- `scalingMember`

## Secure Socket Layer

This feature enables support for Secure Sockets Layer (SSL) connections. The secure HTTPS listener is not started unless the `ssl-1.0` feature is enabled and a keystore is configured.

### Enabling this feature

To enable the Secure Socket Layer feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>ssl-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Secure Socket Layer feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.ssl-1.0; type="osgi.subsystem.feature"
```

## Features that enable this feature

- adminCenter-1.0 - Admin Center
- apiDiscovery-1.0 - API Discovery 1.0
- appSecurity-2.0 - Application Security 2.0
- appSecurityClient-1.0 - Application Security for Client 1.0
- batchManagement-1.0 - Batch Management
- collectiveController-1.0 - Collective Controller
- dynamicRouting-1.0 - Dynamic Routing
- federatedRegistry-1.0 - Federated User Registry
- jcaInboundSecurity-1.0 - Java Connector Architecture 1.0 Security Inflow
- logstashCollector-1.0 - Logstash Collector 1.0
- oauth-2.0 - OAuth
- openidConnectClient-1.0 - OpenID Connect Client
- restConnector-1.0 - JMX REST Connector 1.0
- restConnector-2.0 - JMX REST Connector 2.0
- samlWeb-2.0 - SAML web single sign-on version 2.0
- scim-1.0 - System for Cross-domain Identity Management
- wasJmsSecurity-1.0 - Message Server Security 1.0
- wsAtomicTransaction-1.2 - WS-AT Service
-  zosConnect-1.0 - z/OS Connect
-  zosConnect-1.2 - z/OS Connect 1.2

## IBM API packages provided by this feature

- com.ibm.websphere.ssl

## SPI packages provided by this feature

- com.ibm.wsspi.ssl

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Secure Socket Layer feature:

- channelfw
- keyStore
- ssl
- sslDefault
- sslOptions
- tcpOptions

## Simple and Protected GSSAPI Negotiation Mechanism

This feature enables web applications to integrate SPNEGO 1.0 for authenticating users instead of, or in addition to, the configured user registry.

## Enabling this feature

To enable the Simple and Protected GSSAPI Negotiation Mechanism feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>spnego-1.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Simple and Protected GSSAPI Negotiation Mechanism feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.spnego-1.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- appSecurity-2.0 - Application Security 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

## Feature configuration elements

You can use the following elements in your server.xml file to configure the Simple and Protected GSSAPI Negotiation Mechanism feature:

- authFilter
- spnego

## Static Cluster Member

This feature allows a collective member to participate in a static cluster.

## Enabling this feature

To enable the Static Cluster Member feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>clusterMember-1.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the Static Cluster Member feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.clusterMember-1.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- collectiveMember-1.0 - Collective Member
- restConnector-1.0 - JMX REST Connector 1.0
- restConnector-2.0 - JMX REST Connector 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

## Features that enable this feature

- scalingMember-1.0 - Scaling Member

## IBM API packages provided by this feature

- com.ibm.websphere.cluster.member

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Static Cluster Member feature:

- `clusterMember`

## System for Cross-domain Identity Management

This feature enables support for invoking User Management API using SCIM REST Services.

### Enabling this feature

To enable the System for Cross-domain Identity Management feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>scim-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the System for Cross-domain Identity Management feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.scim-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- `distributedMap-1.0` - Distributed Map interface for Dynamic Caching
- `federatedRegistry-1.0` - Federated User Registry
- `json-1.0` - JavaScript Object Notation for Java
- `servlet-3.0` - Java Servlets 3.0
- `servlet-3.1` - Java Servlets 3.1
- `ssl-1.0` - Secure Socket Layer

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the System for Cross-domain Identity Management feature:

- `administrator-role`
- `authCache`
- `authentication`
- `authorization-roles`
- `basicRegistry`
- `channelfw`
- `classloading`
- `httpAccessLogging`
- `httpDispatcher`
- `httpEncoding`
- `httpEndpoint`
- `httpOptions`
- `httpProxyRedirect`
- `jaasLoginContextEntry`
- `jaasLoginModule`
- `library`

- ltpa
- mimeTypees
- quickStartSecurity
- tcpOptions
- trustAssociation
- virtualHost

## Timed Operations

This feature enables support for logging warnings when certain operations in the application server are running more slowly than expected.

### Enabling this feature

To enable the Timed Operations feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>timedOperations-1.0</feature>
```

### Supported Java Versions

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Timed Operations feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.timedOperations-1.0; type="osgi.subsystem.feature"
```

### SPI packages provided by this feature

- com.ibm.wsspi.timedoperations

### Feature configuration elements

You can use the following elements in your server.xml file to configure the Timed Operations feature:

- timedOperation

## WS-AT Service

This feature enables support for Atomic Transaction for XML-Based Web Services 2.2.

### Enabling this feature

To enable the WS-AT Service feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>wsAtomicTransaction-1.2</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the WS-AT Service feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.wsAtomicTransaction-1.2; type="osgi.subsystem.feature"
```

### Features that this feature enables

- distributedMap-1.0 - Distributed Map interface for Dynamic Caching
- jaxws-2.2 - Java Web Services 2.2
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1
- ssl-1.0 - Secure Socket Layer
- wab-1.0 - OSGi Web Application Bundles

### SPI packages provided by this feature

- com.ibm.wsspi.webservices.wsat

### Feature configuration elements

You can use the following elements in your `server.xml` file to configure the WS-AT Service feature:

- administrator-role
- authCache
- authentication
- authorization-roles
- basicRegistry
- classloading
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- quickStartSecurity
- transaction
- trustAssociation
- wsAtomicTransaction

### WSSecurity SAML

This feature enables the SAML Assertion in the Web Service Security version 1.1 function.

### Enabling this feature

To enable the WSSecurity SAML feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>wsSecuritySaml-1.1</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the WSSecurity SAML feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.wsSecuritySaml-1.1; type="osgi.subsystem.feature"
```

### Features that this feature enables

- samlWeb-2.0 - SAML web single sign-on version 2.0
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1
- wsSecurity-1.1 - Web Service Security

## Web Response Cache

This feature enables local caching for web responses. It includes the distributedMap feature and performs automatic caching of web application responses to improve response times and throughput. Applications can include a cache-spec.xml file to customize the response caching. The cache may be distributed through addition of a network cache provider such as WebSphere eXtreme Scale.

### Enabling this feature

To enable the Web Response Cache feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>webCache-1.0</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Web Response Cache feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.webCache-1.0; type="osgi.subsystem.feature"
```

### Features that this feature enables

- distributedMap-1.0 - Distributed Map interface for Dynamic Caching
- jsp-2.2 - JavaServer Pages 2.2
- jsp-2.3 - JavaServer Pages 2.3
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1

### IBM API packages provided by this feature

- com.ibm.websphere.command
- com.ibm.websphere.command.web
- com.ibm.websphere.servlet.cache

### SPI packages provided by this feature

- com.ibm.wsspi.cache.web

## Web Service Security

This feature provides support for securing JAX-WS web services using a WS-Security policy.

### Enabling this feature

To enable the Web Service Security feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>wsSecurity-1.1</feature>
```

### Developing a feature that depends on this feature

If you are developing a feature that depends on the Web Service Security feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.wsSecurity-1.1; type="osgi.subsystem.feature"
```

### Features that this feature enables

- appSecurity-2.0 - Application Security 2.0
- jaxws-2.2 - Java Web Services 2.2

## Features that enable this feature

- wsSecuritySaml-1.1 - WSSecurity SAML

## Third party API packages provided by this feature

- org.apache.ws.security
- org.apache.ws.security.action
- org.apache.ws.security.cache
- org.apache.ws.security.components.crypto
- org.apache.ws.security.conversation
- org.apache.ws.security.conversation.dkalgo
- org.apache.ws.security.handler
- org.apache.ws.security.message
- org.apache.ws.security.message.token
- org.apache.ws.security.processor
- org.apache.ws.security.saml
- org.apache.ws.security.saml.ext
- org.apache.ws.security.saml.ext.bean
- org.apache.ws.security.saml.ext.builder
- org.apache.ws.security.spnego
- org.apache.ws.security.str
- org.apache.ws.security.transform
- org.apache.ws.security.util
- org.apache.ws.security.validate

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Web Service Security feature:

- wsSecurityClient
- wsSecurityProvider

## WebRTC Rtcomm Gateway

This feature allows the Rtcomm framework to connect with SIP networks.

## Enabling this feature

To enable the WebRTC Rtcomm Gateway feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>rtcommGateway-1.0</feature>
```

## Developing a feature that depends on this feature

If you are developing a feature that depends on the WebRTC Rtcomm Gateway feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.rtcommGateway-1.0; type="osgi.subsystem.feature"
```

## Features that this feature enables

- rtcomm-1.0 - Real-Time Communications
- servlet-3.0 - Java Servlets 3.0
- servlet-3.0 - Java Servlets 3.0

- servlet-3.1 - Java Servlets 3.1
- sipServlet-1.1 - SIP Servlet

## **z/OS Connect**

This feature provides a gateway between mobile, cloud, and web clients and z/OS back-end systems such as CICS Transaction Server, IMS, and batch applications. It provides RESTful APIs and accepts and returns JSON payloads. The feature enables communication with back-end systems by providing a data transformation service that converts JSON payloads to/from byte arrays consumable by z/OS native-language applications written in Cobol, PL/I, and C.

### **Enabling this feature**

To enable the z/OS Connect feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>zosConnect-1.0</feature>
```

### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the z/OS Connect feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.zosConnect-1.0; type="osgi.subsystem.feature"
```

### **Features that this feature enables**

- distributedMap-1.0 - Distributed Map interface for Dynamic Caching
- json-1.0 - JavaScript Object Notation for Java
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1
- ssl-1.0 - Secure Socket Layer

### **SPI packages provided by this feature**

- com.ibm.wsspi.zos.connect

### **Feature configuration elements**

You can use the following elements in your server.xml file to configure the z/OS Connect feature:

- administrator-role
- auditInterceptor
- authCache
- authentication
- authorization-roles
- authorizationInterceptor
- basicRegistry
- classloading
- fileSystemloggerInterceptor
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- quickStartSecurity
- trustAssociation

- zosConnectDataXform
- zosConnectInterceptors
- zosConnectManager
- zosConnectService

## **z/OS Connect 1.2**

This feature provides a gateway between mobile, cloud, and web clients and z/OS back-end systems such as CICS Transaction Server, IMS, and batch applications. It provides RESTful APIs and enables you to route HTTP requests to remote REST endpoints. It also accepts and returns JSON payloads and communicates with back-end systems by providing a data transformation service that converts JSON payloads to/from byte arrays consumable by z/OS native-language applications written in Cobol, PL/I, and C.

### **Enabling this feature**

To enable the z/OS Connect 1.2 feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>zsoConnect-1.2</feature>
```

### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the z/OS Connect 1.2 feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.zosConnect-1.2; type="osgi.subsystem.feature"
```

### **Features that this feature enables**

- distributedMap-1.0 - Distributed Map interface for Dynamic Caching
- jaxrsClient-2.0 - Java RESTful Services Client 2.0
- json-1.0 - JavaScript Object Notation for Java
- servlet-3.0 - Java Servlets 3.0
- servlet-3.1 - Java Servlets 3.1
- ssl-1.0 - Secure Socket Layer

### **SPI packages provided by this feature**

- com.ibm.wsspi.zos.connect

### **Feature configuration elements**

You can use the following elements in your server.xml file to configure the z/OS Connect 1.2 feature:

- administrator-role
- auditInterceptor
- authCache
- authentication
- authorization-roles
- authorizationInterceptor
- basicRegistry
- classloading
- fileSystemloggerInterceptor
- jaasLoginContextEntry
- jaasLoginModule

- library
- ltpa
- quickStartSecurity
- trustAssociation
- zosConnectDataXform
- zosConnectInterceptors
- zosConnectManager
- zosConnectService
- zosConnectServiceRestClient
- zosConnectServiceRestClientBasicAuth

## **z/OS Optimized Local Adapters**

This feature enables high-performance calling between native-language applications on z/OS and business logic in a Liberty profile server environment.

### **Enabling this feature**

To enable the z/OS Optimized Local Adapters feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>zosLocalAdapters-1.0</feature>
```

### **Supported Java Versions**

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the z/OS Optimized Local Adapters feature, include the following item in the `Subsystem-Content` header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.zosLocalAdapters-1.0; type="osgi.subsystem.feature"
```

### **Features that this feature enables**

- `ejbLite-3.1` - Enterprise JavaBeans Lite 3.1
- `ejbLite-3.2` - Enterprise JavaBeans Lite 3.2
- `jca-1.6` - Java Connector Architecture 1.6
- `jca-1.7` - Java Connector Architecture 1.7
- `jndi-1.0` - Java Naming and Directory Interface
-  `zosSecurity-1.0` - z/OS SAF Integration

### **IBM API packages provided by this feature**

- `com.ibm.websphere.ola`

### **Feature configuration elements**

You can use the following elements in your `server.xml` file to configure the z/OS Optimized Local Adapters feature:

- `channelfw`
- `classloading`
- `tcpOptions`

- transaction
- zosLocalAdapters

## **z/OS SAF Integration**

This feature enables the server to use the SAF Registry in the z/OS platform for authenticating users and authorizing access to applications.

### **Enabling this feature**

To enable the z/OS SAF Integration feature, add the following element declaration inside the featureManager element in your server.xml file:

```
<feature>zosSecurity-1.0</feature>
```

### **Supported Java Versions**

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the z/OS SAF Integration feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.zosSecurity-1.0; type="osgi.subsystem.feature"
```

z/OS

### **Features that enable this feature**

-  zosLocalAdapters-1.0 - z/OS Optimized Local Adapters

### **IBM API packages provided by this feature**

- com.ibm.websphere.security.auth.callback

### **Feature configuration elements**

You can use the following elements in your server.xml file to configure the z/OS SAF Integration feature:

- administrator-role
- authCache
- authentication
- classloading
- jaasLoginContextEntry
- jaasLoginModule
- library
- ltpa
- safAuthorization
- safCredentials
- safRegistry
- safRoleMapper

## **z/OS Transaction Management**

This feature enables the application server to synchronize and appropriately manage transactional activity between the Resource Recovery Services (RRS), the transaction manager of the application server, and the resource manager.

### **Enabling this feature**

To enable the z/OS Transaction Management feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>zosTransaction-1.0</feature>
```

### **Supported Java Versions**

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the z/OS Transaction Management feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.zosTransaction-1.0; type="osgi.subsystem.feature"
```

### **Feature configuration elements**

You can use the following elements in your `server.xml` file to configure the z/OS Transaction Management feature:

- `classloading`
- `nativeTransactionManager`
- `transaction`

## **z/OS Workload Management**

This feature provides access to z/OS native workload management (WLM) services. Configuration can be used to classify HTTP traffic in the server so that it can be managed by WLM along with other work in the system.

### **Enabling this feature**

To enable the z/OS Workload Management feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>zosWlm-1.0</feature>
```

### **Supported Java Versions**

- JavaSE-1.6
- JavaSE-1.7
- JavaSE-1.8

### **Developing a feature that depends on this feature**

If you are developing a feature that depends on the z/OS Workload Management feature, include the following item in the Subsystem-Content header in the feature manifest file for your new feature:

```
com.ibm.websphere.appserver.zosWlm-1.0; type="osgi.subsystem.feature"
```

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the z/OS Workload Management feature:

- `channelfw`
- `classloading`
- `httpAccessLogging`
- `httpDispatcher`
- `httpEncoding`
- `httpEndpoint`
- `httpOptions`
- `httpProxyRedirect`
- `mimeTypes`
- `tcpOptions`
- `virtualHost`
- `wlmClassification`
- `zosWorkloadManager`

---

## Liberty Kernel

The kernel

### IBM API packages provided by this feature

- `com.ibm.websphere.config.mbeans`
- `com.ibm.websphere.logging`
- `com.ibm.websphere.logging.hpel`
- `com.ibm.websphere.logging.hpel.reader`
- `com.ibm.websphere.logging.hpel.reader.filters`
- `com.ibm.websphere.logging.hpel.writer`

### SPI packages provided by this feature

- `com.ibm.websphere.crypto`
- `com.ibm.websphere.ras`
- `com.ibm.websphere.ras`
- `com.ibm.websphere.ras.annotation`
- `com.ibm.websphere.ras.annotation`
- `com.ibm.ws.ffdc`
- `com.ibm.ws.ffdc`
- `com.ibm.wsspi.config`
- `com.ibm.wsspi.kernel.filemonitor`
- `com.ibm.wsspi.kernel.service.location`
- `com.ibm.wsspi.kernel.service.utils`
- `com.ibm.wsspi.logging`
- `com.ibm.wsspi.logging`
- `com.ibm.wsspi.security.crypto`
- `com.ibm.wsspi.threading`
- `org.eclipse.equinox.log`

- org.eclipse.osgi.framework.console
- org.eclipse.osgi.framework.eventmgr
- org.eclipse.osgi.framework.log
- org.eclipse.osgi.service.datalocation
- org.eclipse.osgi.service.debug
- org.eclipse.osgi.service.environment
- org.eclipse.osgi.service.localization
- org.eclipse.osgi.service.resolver
- org.eclipse.osgi.service.runnable
- org.eclipse.osgi.service.security
- org.eclipse.osgi.service.urlconversion
- org.eclipse.osgi.signedcontent
- org.eclipse.osgi.storagemanager
- org.eclipse.osgi.util
- org.osgi.service.cm
- org.osgi.service.component
- org.osgi.service.coordinator
- org.osgi.service.event
- org.osgi.service.log
- org.osgi.service.metatype

## Feature configuration elements

You can use the following elements in your `server.xml` file to configure the Liberty Kernel feature:

- config
- executor
- featureManager
- fileset
- include
- logging
- variable
- zosLogging

---

## Liberty: Liberty Repository



8.5.5.2

The Liberty Repository provides an online mechanism to deliver Liberty and additional content, enabling a single point of access for various asset types. The Liberty Repository provides early access to supported new content, including new product capabilities, when they are delivered, rather than waiting for a new release.

The Liberty Repository also enables fast and simple integration with open source, more refined access to runtime capabilities, and quick access to configuration and administration resources for developers and operations teams.

**Important:** Product documentation that is marked with the  icon indicates information about assets that are available only from the Liberty Repository.

## Assets

Asset types available from the Liberty Repository are as follows:

### *Addons*

Artifacts that are packaged to add new capabilities over an existing Liberty installation.

### *Admin Scripts*

Sample scripts for common Liberty administrative tasks.

### *Config Snippets*

Samples of Liberty server configurations for specific tasks.

### *Features*

Individual units of server functionality that can be installed into the Liberty runtime environment.

### *Open Source Integration*

Artifacts that provide simple Liberty integration with commonly used open source projects.

### *Products*

Simple archive installation packages of the Liberty server runtime environment.

### *Product Samples*

Sample server applications that demonstrate the use of Liberty runtime capabilities.

### *Tools*

Tools to enable development and test of Liberty-based applications and runtime extensions.

## Features

The Liberty Repository enables immediate access to fully supported and production-ready features, without the need to wait for new product releases. The features that you add inherit the same support as your existing installation. For a full list of features that are available from the Liberty Repository, see “Liberty features” on page 826.

8.5.5.6

### Offline access to Liberty Repository assets

In addition to accessing assets in the public, online Liberty Repository, you can create the following types of repositories to enable on-premises or offline access to Liberty Repository assets:

#### **Liberty Asset Repository Service**

An open-source service that you can use to create an on-premises repository that is remotely accessible behind the firewall of an enterprise. To get started with the service, see the WASdev/tool.lars project on GitHub.

#### **Local directory-based repository**

Local directory-based repositories that you create when you download assets by using the **installUtility download** command. For more information about the command, see “Downloading assets using the installUtility command” on page 1400.

You can populate these repositories with your own customized content or download Liberty Repository assets by using the **installUtility download** command. As an alternative to downloading individual assets, you can download and extract a `wlp-featureRepo-<version>.zip` file from IBM Fix Central. The .zip file contains a directory-based repository of all features and addons for the particular fix pack of the Liberty. After you populate the repositories, you can install assets from them by using IBM Installation Manager or the **installUtility install** command.

8.5.5.8

For Version 8.5.5.8 and later, you can use Installation Manager and the **installUtility** command to work with repository assets in an archive file. You can access assets directly from the

wlp-featureRepo-<version>.zip file and your own compressed directory-based repositories without extracting the archives.

## Ways to access the Liberty Repository

You can access the Liberty Repository in the following ways:

### WASdev.net website

You can access the Liberty Repository from the Downloads page on WASdev.net, an IBM developerWorks® website for Java application developers. You can browse and download content, filter by asset type, filter by product edition, and search on asset title, description, or edition.

Click any asset from the results of your search, filters, or both to take you to the asset details page. The asset details page provides an asset summary, a description of the asset, installation instructions, and configuration instructions. Links to related assets are also included with compatibility information.

### Developer tools

The Liberty Repository is integrated in developer tools. These tools allow:

- Installation of the server runtime environment from an archive
- Installation of additional content, including features, samples and open source integrations
- Post-installation content
- Runtime and feature dependency awareness, searching and filtering, and configuration snippet inclusion

### Installers

Assets can be installed from the Liberty Repository by using IBM Installation Manager and command-line utilities.

- IBM Installation Manager: If you have IBM Installation Manager installed, you can download and install assets from the Liberty Repository when you install IBM WebSphere Application Server V8.5.5.2 Liberty or later, or upgrade from a previous version of Liberty. In Version 8.5.5.6 or later, you can also install assets from a local directory-based repository or an instance of the Liberty Asset Repository Service.
- Command-line utilities:
  - **8.5.5.6 installUtility**: Find, obtain information about, and install assets that are in a local directory-based repository, an instance of the Liberty Asset Repository Service, or the public Liberty Repository.
  - **featureManager**: Install a feature from the public Liberty Repository and obtain details of features that are already installed.

For more information on the different methods available for installing Liberty Repository assets, see “Installing Liberty Repository assets” on page 1391.

To access the IBM WebSphere Liberty Repository with limited internet access or through a firewall, ensure that you have access to the following hosts and ports:

- public.dhe.ibm.com on port 443
- asset-websphere.ibm.com on port 443

---

## Liberty profile: Product extension

**8.5.5.0**

You can expand the capability of Liberty by writing product extensions.

You can write your own Liberty features and install them onto an existing Liberty server, or you can package them for delivery to your users.

Liberty provides various System Programming Interfaces (SPIs) that you can use to extend the runtime environment; you can also use more advanced features such as operating the Liberty server from your Java applications programmatically.

## Product extension

A product extension is a directory on disk that is structured like the Liberty installation directory, `${wlp.install.dir}`. It is defined to the Liberty installation through a file in the `${wlp.install.dir}/etc/extensions` directory called `extension-name.properties`. The contents of the product extension directory are then used to extend Liberty. Multiple product extensions can be installed together but they must have unique names; this is enforced through the naming of the properties files. The default product extension location, `${wlp.user.dir}/extension`, does not require a properties file; content under this location is automatically detected and is known to the runtime as the “usr” product extension.

Product extensions usually contain one or more Liberty features but can have any content that extends the Liberty environment, for example scripts or resources.

**Best practice:** **8.5.5.0** Install your product extensions into directories that are not affected by updates to the Liberty environment. For more information, see “What might be modified by applying service or an upgrade?” on page 20.

### 8.5.5.0

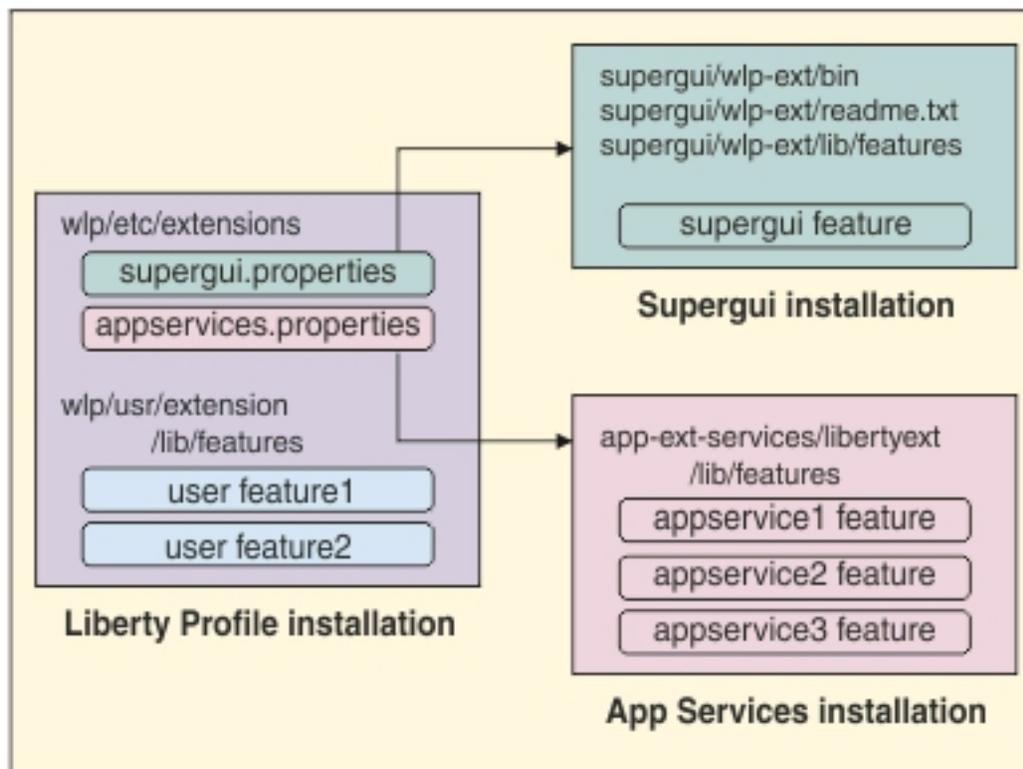


Figure 5.

### 8.5.5.0

The product extension file has the following properties:

```
com.ibm.websphere.productId=your_product_id
com.ibm.websphere.productInstall=absolute_or_relative_file_path
```

**Note:** When a relative file path is used, it must be a peer of the `${wlp.install.dir}` value.

**8.5.5.0**

For example:

```
com.ibm.websphere.productId=org.acme.supergui  
com.ibm.websphere.productInstall=supergui/wlp-ext
```

## Feature

A Liberty feature consists of a definition file (feature manifest), and a collection of OSGi bundles that provide classes and services corresponding to a particular capability in the Liberty runtime environment.

## Scenarios for using a Liberty feature instead of a regular application

Implementing a function as a Liberty feature instead of as an application might be appropriate in a number of scenarios. The following list describes some of the benefits of using a feature:

- Features are controlled through feature manager configuration, so they are separate from user application management.
- Feature code has access to the Liberty SPI, which allows deeper integration with the runtime environment.
- Features can receive user-specified configuration from the `server.xml` file, and expose their configuration settings in the development tools without the tools having to be changed.
- Features can easily expose classes and services to each other and to user applications.
- Features can be extremely lightweight with no application container dependencies.
- Features can be used to augment a particular programming model. For example, a User Feature can add support for custom Blueprint namespace handlers or Blueprint annotations to the OSGi Application programming model.

**Note:** Features cannot generally be directly portable to other application servers; if portability is important you should use specification-compliant applications.

## Developing a simple feature

See “Developing a Liberty feature manually” on page 1771, “Creating a Liberty feature by using developer tools” on page 1782, and “Liberty feature manifest files” on page 1773.

## Using a feature in the server

To use a user-written feature in the Liberty server, you must install it into a product extension directory. This might be the predefined “user product extension” location or an extension that is located outside the Liberty installation directory. Then you can add the feature name into the server configuration.

The user product extension is a predefined directory where the server looks for additional features. The feature definition `.mf` file must be copied into the `${wlp.user.dir}/extension/lib/features` directory and the bundle `.jar` files must be copied into the `${wlp.user.dir}/extension/lib` directory.

User-written features are added to the server configuration in the same way as product features. To avoid name clashes with features from different providers, features that are part of a product extension must be prefixed with the extension name. For features in the `usr/extension/lib` directory, the default prefix is `usr:.`

For example, if you have installed a feature called `simple-1.0` into the `${wlp.user.dir}/extension/lib` directory, you must configure that feature into the `server.xml` as follows:

```
<featureManager>
  <feature>usr:simple-1.0</feature>
</featureManager>
```

If you have installed a feature called `myFeature` into your own location, and defined a product extension in the `#{wlp.install.dir}/etc/extensions/myExt.properties` file, you must configure that feature into the `server.xml` file as follows:

```
<featureManager>
  <feature>myExt:myFeature</feature>
</featureManager>
```

When you start the server, the feature is detected by the feature manager and the bundles are installed into the OSGi framework and started.

See also “Adding and removing Liberty features” on page 1587 and “Liberty: Feature management” on page 824.

## Programmatically using a feature from applications

Features can expose classes and services to applications.

To expose Java classes for application use, you must list the class packages in the `IBM-API-Package` header in the feature manifest. Listing the class packages in the `IBM-API-Package` header makes the classes visible to the application class loaders. Visibility of API packages can be controlled through the API visibility type. See “Specifying API and SPI packages for a Liberty feature project” on page 1784.

To allow services to be used by OSGi applications, you must list them in the `IBM-API-Service` header in the feature manifest. A feature provides OSGi services so that you can refer to those services programmatically from your applications.

Services should generally be registered into the OSGi Service Registry (SR) to allow applications (or other features) to locate them. OSGi applications and other features can perform a direct lookup from the SR, or can use capabilities such as Blueprint or OSGi Declarative Services to inject their service dependencies. Java EE applications are more likely to locate services through JNDI; in Liberty there is a federation of the SR and JNDI that allows Java EE applications to use JNDI to locate services in the SR. For more information, see “Working with the OSGi service registry” on page 1789.

## Exposing a feature as a web application

To expose a Liberty feature as a web application, you can publish the OSGi bundles in the feature as web application bundles (WABs). In addition to the OSGi headers that a bundle requires, you can specify the web application context path by using the `Web-ContextPath` header.

For example:

```
Web-ContextPath: myWABapp
Bundle-ClassPath: WEB-INF/classes
```

## Configuration injection and processing

A major benefit of using features is that they can be easily configured by the user in the `server.xml` file (and included files). The configuration files are monitored and parsed by the Liberty profile kernel and the resulting sets of properties can be injected into the relevant component each time they change.

Liberty configuration is managed by the OSGi Configuration Admin (CA) service in the kernel and can be accessed according to that specification. Sets of configuration properties are identified by a persisted identity (PID) that is used to associate the element in the `server.xml` file with the component that registers to receive the properties.

For example, if you register your feature with the CA service using a PID of `com.acme.console`, a user can specify the following configuration in the `server.xml` file:

```
<com.acme.console color="blue" size="17"/>
```

And your feature will receive the properties:

- `color="blue"`
- `size="17"`

You can optionally provide metadata that describes your configuration properties by using OSGi Metatype descriptors. The use of descriptors causes your configuration metadata to be included in the configuration schema that is generated by Liberty and is used by the Developer Tools, so your configuration properties are automatically presented to application developers as they configure their server.

**8.5.5.0** For more details on receiving and describing configuration properties, see “Enabling a service to receive configuration data” on page 1796.

## Declarative Services in the Liberty

Larger or more complex features often benefit from the use of OSGi Declarative Services (DS) to enable the feature to be composed of multiple services, and to manage the injection of dependencies and configuration properties. The use of DS allows lazy activation of services, deferring the loading of Java classes until the service is used, and ordering the activation of services based on dependencies. Most of the features in the Liberty product are managed by DS.

**8.5.5.0** See also “Composing advanced features by using OSGi Declarative Services” on page 1793.

---

## Liberty: Security

Liberty security provides protection for web resources in accordance with the Servlet 3.0 specification and EJB resources in accordance with the `ejbLite` 3.1 specification. The Liberty security also provides protection for the JMX connections when you are using the REST connector.

The following diagram shows a typical security process involved when accessing a protected web resource. To make the security process work, you must configure the appropriate security features and the configurations that are required for the authentication and authorization.

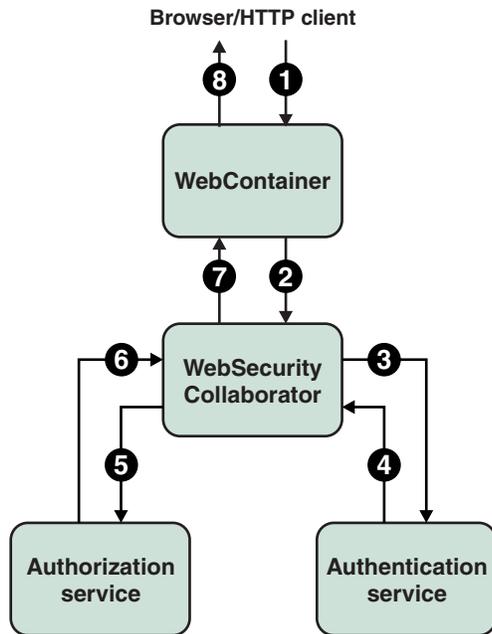


Figure 6. Typical security flow for web resources

1. An HTTP client requests a web resource in the WebContainer.
2. The WebContainer delegates the security check to the WebSecurity Collaborator.
3. The WebSecurity Collaborator prompts the user to enter credentials if absent, and uses the Authentication service to authenticate the user.
4. The Authentication service authenticates, creates, and returns the subject if authenticated successfully. Otherwise, the Authentication service reports an exception for the authentication failure.
5. The WebSecurity Collaborator uses the Authorization service to perform a user authorization check.
6. The Authorization service returns the authorization result to the WebSecurity Collaborator.
7. The WebSecurity Collaborator returns the result of the security check about whether the user is authorized.
8. The WebContainer serves or rejects the requested resource.

The following sections provides a summary of the primary security components in Liberty:

- “Quick start” on page 973
- “Authentication” on page 973
- “Authorization” on page 973
- “Secure Socket Layer (SSL)” on page 973
- “Single Sign-On (SSO)” on page 973
- “Web security-related properties” on page 973
- “Security public APIs” on page 973
- “Management security” on page 974
- **z/OS** “ z/OS® security” on page 974
- “Authentication aliases” on page 974
- “Configuration examples and samples” on page 974
- “Security compatibility and differences” on page 974
- “Configuring Lightweight Directory Access Protocol (LDAP)” on page 974
- “Troubleshooting” on page 975

- **Distributed operating systems** “Tools” on page 975

## Quick start

With the `quickStartSecurity` element, you can configure a single user security environment in Liberty. See “Liberty:Quick overview of security” on page 975 for details of how the security workflow is when you use the `quickStartSecurity` element, and “Getting started with security in Liberty” on page 1829 for a sample task.

## Authentication

Authentication confirms the identity of a user. The most common form of authentication is user name and password, such as through either basic authentication or form login for web applications. When a user is authenticated, the source of a request is represented as a Subject object at the run time. This process involves performing access control checks when a user accesses a resource, based on the authorization rules configured for the resource. See “Liberty:Authentication” on page 976 for more concepts and “Authenticating users in Liberty” on page 1850 for detailed tasks.

## Authorization

Authorization determines whether to grant a user access to resources within the system. The Java EE model uses subjects, resources, and roles to determine what can and cannot be allowed. This process involves checking the user credentials such as the user ID and password, certificates, and tokens, and creating a subject based on the authenticated user. See “Liberty: Authorization” on page 999 for more concepts and “Authorizing access to resources in Liberty” on page 1939 for detailed tasks.

## Secure Socket Layer (SSL)

SSL provides transport level security. See “Enabling SSL communication in Liberty” on page 1834 for detailed tasks.

## Single Sign-On (SSO)

SSO enables access to applications without the user being prompted to login multiple times. See Concept of SSO for more details and “Customizing SSO configuration using LTPA cookies in Liberty” on page 1887 for the detailed task.

## Web security-related properties

There are many configuration properties that you can configure as part of web security, such as SSO and client certificate authentication, for your applications. See for available attributes and see “Configuring web security related properties in Liberty” on page 1994 for some examples.

## Security public APIs

Liberty contains public APIs that you can use to implement security functions. The security public APIs in Liberty are a subset of the traditional security public APIs. The main classes are `WSSecurityHelper`, `WSSubject`, and `RegistryHelper`. These classes contain a subset of the methods that are available in the WebSphere Application Server traditional versions. There is also a new class `WebSecurityHelper`. See “Liberty:Security public APIs” on page 1004.

The Java API documentation for each Liberty API is available in a separate `.zip` file in one of the javadoc subdirectories of the `{wlp.install.dir}/dev` directory.

See “Developing extensions to the Liberty security infrastructure” on page 1998 for some examples.

## Management security

Management security means that you can manage Liberty by using a remote JMX client. To secure remote connections using the REST connector, see “Connecting to Liberty by using JMX” on page 1641. You can also develop your own JMX client application as described in “Developing a JMX Java client for Liberty” on page 1645.

z/OS

## z/OS® security

The System Authorization Facility (SAF) on the z/OS platform is supported in Liberty for authentication and authorization. See “Enabling z/OS authorized services in Liberty for z/OS” on page 1942 and Configuring SAF Authorization for detailed tasks.

## Authentication aliases

Authentication data aliases provide the security support for database connectivity. See “Configuring authentication aliases for Liberty” on page 1997.

## Configuration examples and samples

8.5.5.0

There are several security configuration examples on the WASdev.net website for reference when configuring security for your applications on Liberty.

## Security compatibility and differences

You can learn about the main differences in the security capability between the traditional and Liberty. See “Configuration differences between the traditional and Liberty: security” on page 1008.

## Configuring Lightweight Directory Access Protocol (LDAP)

After selecting the LDAP User Registry item to add to the server configuration, the **LDAP User Registry Details** panel will display a list for the supported LDAP server types. If you select a supported LDAP server type, the LDAP filters associated with the selected LDAP server type will not automatically pre-populated.

Each of the supported LDAP server types has a default set of filters defined. After the **LDAP User Registry** item and server type has been added, the associated LDAP filters can be configured by selecting the **LDAP User Registry** configuration and adding the required LDAP filter:

- Active Directory LDAP filters
- Custom LDAP filters
- Domino LDAP filters
- eDirectory LDAP filters
- IBM Directory Server LDAP filters
- iPlanet LDAP filters
- Netscape LDAP filters
- SecureWay LDAP filters

Selecting any of the LDAP filters will display the default values for the filter types:

- user filter
- group filter
- user ID map
- group ID map

- group member ID map

If the default filters are used, the `server.xml` file is not updated with any filter information. If any of the filters are changed, only the changed filter types will be updated in the `server.xml`.

**Note:** If you do not specify or select a reference ID using the **Browse** button, the default filters associated with selected LDAP server type will be used.

Alternatively, you can add an LDAP filter to the server configuration. An ID must be specified to associate the reference to this particular filter configuration, in order to associate it with the LDAP User Registry configuration. If this method of configuring the LDAP filters is used, the reference ID will then be selected on the **LDAP User Registry Details** panel (located using the **Browse** button under the respective LDAP filter type).

If you are using Eclipse-based developer tools to configure LDAP, verify the configuration saved against the samples in `wlp/templates/config/ldapRegistry.xml`.

For more information, see “Configuring LDAP user registries in Liberty” on page 1852.

## Troubleshooting

Use the troubleshooting information to solve security-related problems when you use Liberty. See “Troubleshooting security” on page 2298 and “Troubleshooting LDAP” on page 2300.

### Distributed operating systems

## Tools

Configure security by using the Eclipse-based developer tools for Liberty. See “Editing the Liberty configuration by using developer tools” on page 1556. Specific information about tools and security configuration is available in “Configuring TAI on Liberty by using developer tools” on page 1891 and “Configuring JAAS on Liberty by using developer tools” on page 1870.

## Liberty:Quick overview of security

To understand the basic workflow of security in Liberty, some common security terms are detailed along with an example.

### Security key terms

#### Authentication

Authentication confirms the identity of a user. The most common form of authentication is user name and password, such as through basic authentication or form login for web applications. When a user is authenticated, the source of a request is represented as a Subject object at run time.

#### Authorization

Authorization determines whether a user has access to a given role within the system. The Java EE model uses subjects, roles, and role mappings to determine if access is allowed.

**Role** A role is defined within the Java EE application. Some roles, such as the Administrator role, are predefined by the system. Other roles are defined by the application developer. In Java EE, subjects are usually granted or denied access to a role based on the roles they perform within the application.

#### Subject

A subject is both a general term and a Java object: `javax.security.auth.Subject`. Generally, the term subject means active entities within the system, such as users on the system, and even the system process itself.

## Security workflow example

The following example demonstrates how the security is applied when a user requests access to a resource. For example, a user Bob wants to access a servlet `myWebApp`. See the code samples in “Getting started with security in Liberty” on page 1829.

To access the servlet `myWebApp`, the following conditions must be true:

1. Bob must be able to log in to the system because the servlet is protected.
2. Bob must be in the `testing` role because the servlet is restricted by using an `auth-constraint` element in the deployment descriptor.

If Bob cannot log in to the system, or Bob is not in the `testing` role, then the access to the servlet `myWebApp` is denied.

Another user Alice can log in to the system because Alice is a valid user. But Alice is not in the `testing` role. An HTTP 403 error (Access Denied/Forbidden) displays when Alice logs in.

## Liberty:Authentication

Authentication in the Liberty security is to confirm the identity of a user.

To access a protected web resource, the user must provide credential data, such as user ID and password. The authentication process involves collecting this user credential information (based on how the web application was configured to collect this data) and validating it against the configured registry. When the credential information is verified, a JAAS subject is created for that user. The subject contains additional information about the user, such as the groups that the user belongs to, and the tokens created for the user. The information in this subject is then used during the authorization process to determine whether the user can access the resource.

The following diagram illustrates a typical authentication process flow for a web resource.

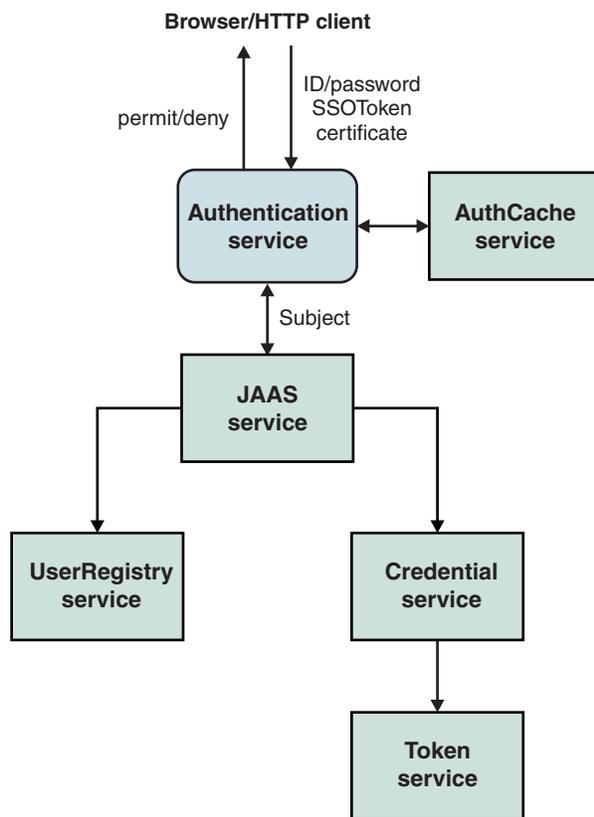


Figure 7. Overview of authentication process

The authentication process involves gathering credential data from the user, checking the cache to see whether the subject exists for that user and in its absence calling the JAAS service to perform the authentication to create a subject. The JAAS service calls a set of login modules to handle the authentication. One or more of the login modules creates the subject depending on the credential data. The login module then calls the registry that is configured to validate the credential information. If the validation is successful, the authentication process collects and creates relevant information for that user, including the groups that the user belongs to and the single sign-on (SSO) token used for SSO capability, and stores them in the subject as relevant credentials. You can also customize the information saved in the subject by plugging in custom login modules during this process.

When the authentication is successful, the SSO token that is created during the process is sent back to the browser in a cookie. The default name of the configurable cookie is `ltpaToken2`. On subsequent calls, the token information is used to authenticate the user. If this authentication fails, the authentication service tries to use other authentication data, such as the user ID and password, if they still exist in the request.

**Note:** To support user IDs and passwords that contain non US-ASCII characters, form login method is required for web applications. For more information, see `autoRequestEncoding` and `autoResponseEncoding`.

The following sections describe these concepts in detail:

- “User registries” on page 978
- “Authentication cache” on page 978
- “JAAS configuration” on page 978
- “JAAS login modules” on page 979

- “Callback handler” on page 980
- “Credentials and tokens” on page 980
- “LTPA” on page 980
-  **8.5.5.5** “SPNEGO” on page 981
-  **8.5.5.8** “Kerberos constrained delegation for SPNEGO” on page 982
- “Single sign-on (SSO)” on page 982
-  **8.5.5.7** “SAML Web Browser SSO” on page 982
- “Pluggable authentication” on page 983
- “Identity assertion” on page 983
- “RunAs() authentication” on page 984
- “Proxy login module” on page 984
- “Certificate login” on page 985
- “Hash table login module” on page 985

## User registries

When validating the authentication data of a user, the login modules call the user registry that is configured to validate the user information. Liberty supports both a simple configuration-based user registry and a more robust LDAP-based registry. For more information, see “Configuring a user registry for Liberty” on page 1851.

**8.5.5.0** Using the LDAP registry, you can also federate multiple repositories and execute the LDAP operations on two or more registries. The Liberty user can configure the LDAP registry federation feature either directly in the `server.xml` file or can configure in the **LDAP Registry Federation** section in the developer tool. After the configuration of the federated repositories, you can obtain a consolidated result of the federated repositories on any operation that you want to perform. For example, if you want to perform a search operation for all user names that starts with *test*, you can perform a search across the set of LDAP registries and get the consolidated search result which can then be sent back to the calling program.

## Authentication cache

Because creating a subject is relatively expensive, Liberty provides an authentication cache to store a subject after the authentication of a user is successful. The default expiration time for the cache is 10 minutes. If the user does not log back in within 10 minutes, the subject is removed and the process of authentication repeats to create a subject for that user. Changes to the configuration that affect the creation of the subject, such as adding a login module or changing the LTPA keys, will cause the authentication cache to be cleared. If the subject is cached and the information in the registry changes, the cache is updated with the information in the registry. You can configure the cache timeout period, and the cache size, and you can also disable or enable caching. For more information, see “Configuring the authentication cache in Liberty” on page 1867.

## JAAS configuration

JAAS configuration defines a set of login modules to create the subject. Liberty supports the following JAAS configurations:

### **system.WEB\_INBOUND**

Used when accessing web resources such as servlets and JSPs.

### **WSLogin**

Used by applications when using the programmatic login. It is also used by applications running

in an application client container, but unlike the `ClientContainerJAAS` configuration, it does not recognize the `CallbackHandler` handler that is specified in the client application module's deployment descriptor.

#### **system.DEFAULT**

Used for login when no JAAS configuration is specified.

#### **8.5.5.4 system.DESERIALIZE\_CONTEXT**

Used when a security context is being deserialized. This JAAS configuration handles authentication to re-create the subjects that were active on the thread at the time the security context was serialized. You can specify this JAAS configuration and add your own custom JAAS login modules by editing the JAAS configuration entry in the `server.xml` file to ensure that the propagated subjects contain your custom information.

#### **8.5.5.6 ClientContainer**

Used by applications running in an application client container. This JAAS login configuration recognizes the `CallbackHandler` handler that is specified in the client application module's deployment descriptor, if one is specified.

The `system.WEB_INBOUND` and `system.DEFAULT` configurations have these default login modules in this order: **hashtable**, **userNameAndPassword**, **certificate**, and **token**. The `WSLogin` configuration has the proxy login module as the default login module, and the proxy delegates all the operations to the real login module in `system.DEFAULT`.

No explicit configuration is required unless you want to customize by using the custom login modules. Depending on the requirement, you can customize specific login configurations. For example, if you want all the web resource logins to be customized, you must add custom login modules only to the `system.WEB_INBOUND` configuration. See “Configuring a JAAS custom login module for Liberty” on page 1868.

## **JAAS login modules**

JAAS configuration uses a set of login modules to create the subject. Liberty provides a set of login modules in each of the login configurations. Depending on the authentication data, a particular login module creates the subject. The authentication data is passed to the login modules by using the callback handler, as specified in the JAAS specification. For example, if the user ID and password callback handler is being used for authentication, the **userNameAndPassword** login module handles the authentication. If a `SingleSignOnToken` credential is presented as the authentication data, only the **token** login module handles the authentication.

The following default login modules are supported in Liberty:

#### **userNameAndPassword**

Handles the authentication when user name and password are used as the authentication data.

#### **certificate**

Handles the authentication when an X509 certificate is used as the authentication data of mutual SSL.

**token** Handles the authentication when an SSO token is presented as the authentication data. During the authentication process, an SSO token is created and sent back to the HTTP client (browser) in a cookie. On subsequent requests, this cookie is sent back by the browser and the server extracts the token from the cookie to authenticate the user when the single sign-on is enabled.

#### **hashtable**

Used when the authenticated data is sent through a predefined hash table. For more information about the hash table login, see “Hash table login module” on page 985. This login module is also used by the security run time when authentication is performed using identity only; for example, in the case of `runAs`.

**proxy** The default login module for WSLLogin. See “Proxy login module” on page 984.

The login modules are called in the order that they are configured. The default order is **hashtable**, **userNameAndPassword**, **certificate**, **token**. If you must customize the login process by using custom login modules, you can provide them and configure them in the order you need. Typically, place a custom login module first in the list of login modules so that it is called first. When a custom login module is used, you must specify all the login module information in the configuration along with the custom login module in the required order.

When a login module determines that it can handle the authentication, it first makes sure that the authentication data that is passed in is valid. For example, for user name and password authentication, the configured user registry is called to verify the authentication information. For token authentication, the token must be decrypted and valid for the verification to succeed.

When the authentication data is validated, the login modules create credentials with additional data for the user including the groups and the SSO token. A custom login module can add additional data to the subject by creating its own credentials. For the Liberty authorization to work, the subject must contain the `WSCredential`, `WSPrincipal`, and `SingleSignonToken` credentials. The `WSCredential` credential contains the groups information, with additional information that is required by the security runtime environment.

## Callback handler

The Liberty supports various callback handlers for providing data to the login modules during the JAAS authentication process. A custom login module can use the callback handler information to authenticate itself. For example, if the callback handler needs to access some information in an `HttpServletRequest` object, it can do so by using that specific callback handler.

The following callback handlers and factories for programmatic JAAS login are supported in Liberty:

- `com.ibm.websphere.security.auth.callback.WSCallbackHandlerImpl`
- `com.ibm.wsspi.security.auth.callback.WSCallbackHandlerFactory`

The Java API documentation for each Liberty API is available in a separate `.zip` file in one of the javadoc subdirectories of the `{wlp.install.dir}/dev` directory.

See “Developing JAAS custom login modules for a system login configuration” on page 2002.

## Credentials and tokens

As mentioned in the `loginModule` section, credentials are created as part of the subject creation process. Liberty creates the `WSCredential`, `SingleSignonToken`, and `WSPrincipal` credentials. The `SingleSignonToken` credential contains the token that is sent back to the browser in a cookie for SSO to work. This token contains the user information and an expiration time. It is signed and encrypted by using the Lightweight Third Party Authentication (LTPA) keys that are generated during the first server startup. The default expiration time is 2 hours and is an absolute time, not based on user activities. After the 2 hours, the token expires and the user must log in again to access the resource.

## LTPA

LTPA is intended for distributed and multiple application server environments. In Liberty, LTPA supports SSO and security in a distributed environment through cryptography. This support enables LTPA to encrypt, digitally sign, and securely transmit authentication-related data, and later decrypt and verify the signature.

Application servers can securely communicate using the LTPA protocol. The protocol also provides the SSO feature, whereby a user is required to authenticate only when connecting to a domain name system

(DNS). Then the user can access resources in other Liberty servers in the same domain without getting prompted. The realm names on each system in the DNS domain are case-sensitive and must match identically.

The LTPA protocol uses cryptographic keys to encrypt and decrypt user data that passes between the servers. These keys must be shared between different servers for the resources in one server to access resources in other servers, assuming that all the servers involved use the same user registry. LTPA requires that the configured user registry must be a centrally shared repository so that users and groups are the same, regardless of the server.

When using LTPA, a token is created that contains the user information and an expiration time, and is signed by the keys. The LTPA token is time sensitive. All participating servers must have their time and date synchronized. If not, LTPA tokens are prematurely expired and cause authentication or validation failures. Coordinated Universal Time (UTC) is used by default, and all other servers must have the same UTC time. See your operating system documentation for information about how to ensure the same UTC time among servers.

The LTPA token passes to other servers through cookies for web resources when SSO is enabled.

If the receiving servers use the same keys as the originating server, the token can be decrypted to obtain the user information, which then is validated to make sure that the token is not expired and that the user information in the token is valid in its registry. On successful validation, the resources in the receiving servers are accessible after the authorization check.

Each server must have valid credentials. When the credentials expire, the server is required to communicate to the user registry to authenticate. Extending the time that the LTPA token remains cached presents a slightly increased security risk to be considered when defining your security policies.

If key sharing is required between different Liberty servers, copy the keys from one server to another. For security purposes, the keys are encrypted with a randomly-generated key, and a user-defined password is used to protect the keys. This same password is needed when importing the keys into another server. The password is used only to protect the keys, and is not used to generate the keys.

When security is enabled, LTPA is configured by default during the Liberty server start time. For more information about the LTPA support, see “Configuring LTPA in Liberty” on page 1872.



8.5.5.5

## SPNEGO

Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) enables users to log in to the Microsoft Domain controller once and access protected applications on Liberty servers without getting prompted again.

When SPNEGO web authentication is enabled, and the browser client accesses a protected resource on the Liberty server, SPNEGO is responsible for authenticating access to the secured resource that is identified in the HTTP request. The browser client creates a SPNEGO token and sends it to the Liberty server as part of the HTTP request. The WebSphere Application Server validates and retrieves the user identity from the SPNEGO token. The identity is used to establish a secure context between the user and the application server.

For more information about SPNEGO, see  8.5.5.5 SPNEGO. For further information on configuring SPNEGO on the Liberty server, see  8.5.5.5 Configuring SPNEGO authentication in Liberty.



8.5.5.8

## Kerberos constrained delegation for SPNEGO

The Kerberos constrained delegation feature provides two APIs that are used to create out-bound SPNEGO tokens for back end services that support SPNEGO authentication, such as .NET servers and other Liberty servers.

The Kerberos v5 extension called S4U (Services for Users) comprises two parts:

### S4U2self

Allows a Liberty server to obtain a service ticket to itself on behalf of a user. This can be used with any form of authentication that is supported by Liberty. S4U2self is the Kerberos Protocol Transition extension.

### S4U2proxy

Allows a Liberty server to obtain service tickets to trusted services on behalf of a user. These service tickets are obtained by using the user's service ticket to the Liberty service. The services are constrained by the Kerberos Key Distribution Center (KDC) administrator. S4U2proxy is the Kerberos Constrained Delegation extension.

## Single sign-on (SSO)

SSO enables users to log in in one place (one server for example) and access applications on other servers without getting prompted again. To make SSO work, the LTPA keys must be exchanged across different Liberty servers, the user registries must be the same, and the token must not have expired. To exchange the LTPA keys, you can copy the `ltpa.keys` file from one server to another and restart the server to use the new LTPA keys. The registries that are used by all the servers participating in the SSO domain must be the same.

When a user is authenticated in one Liberty server, the SSO token created for the user during the authentication process is put in the cookie that is sent to the HTTP client, for example a browser. If there is another request from that client to access another set of applications on a different server, but in the same DNS that was configured as part of the SSO configuration in the first server, the cookie is sent along with the request. The receiving server tries to authenticate the user using the token in the cookie. If both conditions are met, the receiving server validates the token and creates a subject based on the user in this server, without prompting the user to log in again. If the token cannot be validated (for example, it cannot decrypt or verify the token because of LTPA key mismatch), the user is prompted to enter the credential information again.

Any application that is configured to use the `Form-login` attribute must have SSO to be configured for that server. When the user is authenticated for a `form-login`, the token is sent back to the browser that will be used for authorizing the user when the resource is accessed.

See “Customizing SSO configuration using LTPA cookies in Liberty” on page 1887.



8.5.5.7

## SAML Web Browser SSO

SAML Web Browser SSO enables web applications to delegate user authentication to a SAML identity provider instead of a configured user registry.

For further information on configuring SAML Web Browser SSO on the Liberty server, see “SAML 2.0 Web Browser Single-Sign-On” on page 994.

## Pluggable authentication

Use the following ways to customize the authentication process:

- Provide a custom login module. Most of the authentication process is built around JAAS login modules, so you can plug in custom login modules before, after, or between the login modules provided by Liberty. See “Configuring a JAAS custom login module for Liberty” on page 1868.
- Implement Trust Association Interceptor (TAI) to handle all web resource-based authentication. See “Developing a custom TAI for Liberty” on page 1998.

For more details about the JAAS login module and TAI, see Advanced authentication in WebSphere Application Server.

## Identity assertion

Besides authentication that requires a requesting entity to prove its identity, Liberty also supports identity assertion. This is a relaxed form of authentication that does not require identity proof, but rather accepts the identity based on a trust relationship with the entity that vouches for the asserted identity.

Use the following ways to assert identities in Liberty

1. Use the hash table login. See “Developing JAAS custom login modules for a system login configuration” on page 2002.
2. Use `IdentityAssertionLoginModule`. You can allow an application or system provider to assert an identity with trust validation. To use `IdentityAssertionLoginModule`, use the JAAS login framework, where trust validation is accomplished in one custom login module and credential creation is accomplished in `IdentityAssertionLoginModule`. You can use the two login modules to create a JAAS login configuration that can be used to assert an identity.

The following two custom login modules are required:

### User implemented login module (trust validation)

The user implemented login module performs whatever the user requires in trust verification. When trust is verified, the trust verification status and the login identity must be put into a map in the share state of the login module, so that the credential creation login module can use the information. Store this map in the following property:

```
com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.state
```

This property consists of the following properties:

- `com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.trusted`

This property is set to true if trusted and false if not trusted.

- `com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.principal`

This property contains the principal of the identity.

- `com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.certificates`

This property contains the certificate of the identity.

### Identity assertion login module (credential creation)

The following module creates the credential:

```
com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule
```

This module relies on the trust state information in the shared state of the login context.

The identity assertion login module looks for the trust information in the shared state property:

```
com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.state
```

This property contains the trust status and the identity to log in, and must include the following property:

- ```
com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.trusted
```

This property is set to true when trusted and false when not trusted.

- ```
com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.principal
```

This property contains the principal of the identity to log in if a principal is used.

- ```
com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.certificates
```

This property contains an array of a certificate chain that contains the identity to log in if a certificate is used.

A `WSLoginFailedException` message is returned if the state, trust, or identity information is missing. The login module then logs in with the identity, and the subject contains the new identity.

See “Customizing an application login to perform an identity assertion by using JAAS” on page 2013.

## RunAs() authentication

When you have successfully authenticated after calling a servlet, the servlet can make subsequent calls, for example to other servlets. These subsequent calls are normally made under the same security identity that you originally used to log in to the servlet. This identity is known as the caller identity. Alternatively, you can choose to delegate to a different identity by using the `RunAs` specification, so that any subsequent calls that the servlet makes run under this other identity. To summarize, you have two options to propagate the security identity:

- Propagate the caller identity, which is the default behavior.
- Delegate to the `RunAs` identity that you can specify by using the `RunAs` specification.

After the server authenticates the original user, the server then authenticates the `RunAs` user. If this authentication fails, the server falls back to propagate the caller identity.

To use the `RunAs` specification, you must update the deployment descriptor of your application to include the `run-as` element or `@RunAs` annotation. Set this element to the security role that you want to delegate to.

See “Configuring `RunAs` authentication in Liberty” on page 1888.

## Proxy login module

The proxy login module class loads the application server login module and delegates all the operations to the real login module implementation. The real login module implementation is specified as the `delegate` option in the option configuration. The proxy login module is required because the application class loaders do not have visibility of shared library class loaders of the application server product. With an application programmatic login that uses the `Login()` method of the `LoginContext` class with JAAS login context entry `WSLogin`, the proxy login module delegates all the work to the JAAS login context entry `system.DEFAULT`.

## Certificate login

With the certificate login feature, you can authenticate web requests such as servlets by using client side X509 certificates instead of supplying a user ID and password.

Certificate authentication works by associating a user in the user registry with the distinguished name in the client certificate of a web request. Trust is established by having the client certificate trusted by the server, for example the signer of the client certificate must be in the trust store of the server. This mechanism eliminates the need for users to supply a password to establish trust.

See “Securing communications in Liberty” on page 1833.

## Hash table login module

Look up the required attributes from the user registry, put the attributes in a hash table, and then add the hash table to the shared state. If the identity is switched in this login module, you must add the hash table to the shared state. If the identity is not switched, but the value of the `requiresLogin` code is true, you can create the hash table of attributes. You do not have to create a hash table in this situation, because Liberty handles the login for you. However, you might consider creating a hash table to gather attributes in special cases. For example, if you are using your own special user registry, then creating a `UserRegistry` implementation, using a hash table, and letting the server gather the user attributes for you, might be a simple solution.

The following rules define in more details about how a hash table login is completed. You must use a `java.util.Hashtable` object in either the Subject (public or private credential set) or the shared-state `HashMap`. The `com.ibm.wsspi.security.token.AttributeNameConstants` class defines the keys that contain the user information. If the `Hashtable` object is put into the shared state of the login context using a custom login module that is listed before the hashtable login module, the value of the `java.util.Hashtable` object is searched using the following key within the shared-state `hashMap`:

### Property

`com.ibm.wsspi.security.cred.propertiesObject`

### Reference to the property

`AttributeNameConstants.WSCREDENTIAL_PROPERTIES_KEY`

### Explanation

This key searches for the `Hashtable` object that contains the required properties in the shared state of the login context.

### Expected result

A `java.util.Hashtable` object.

If a `java.util.Hashtable` object is found inside the Subject or within the shared state area, verify that the following properties are present in the hash table:

- `com.ibm.wsspi.security.cred.uniqueId`

### Reference to the property

`AttributeNameConstants.WSCREDENTIAL_UNIQUEID`

### Returns

`java.util.String`

### Explanation

The value of the property must be a unique representation of the user. For the Liberty default implementation, this property represents the information that is stored in the application authorization configuration. The information is in the application deployment descriptor after it is deployed and the user-to-role mapping is performed. See the expected format examples if the user to role mapping is performed by looking up a user registry implementation of Liberty.

## Expected format examples

Table 7. Format examples for `uniqueId`. This table gives expected format examples.

| User Registry | Format (UniqueUserId) value                  |
|---------------|----------------------------------------------|
| LDAP          | ldapRegistryRealm/cn=kevin,o=mycompany,c=use |
| Basic         | basicRegistryRealm/kelvin                    |

The `com.ibm.wsspi.security.cred.uniqueId` property is required.

- `com.ibm.wsspi.security.cred.securityName`

### Reference to the property

`AttributeNameConstants.WSCREDENTIAL_SECURITYNAME`

### Returns

`java.util.String`

### Explanation

This property searches for **securityName** of the authentication user. This name is commonly called the display name or short name. Liberty uses the **securityName** attribute for the `getRemoteUser`, `getUserPrincipal`, and `getCallerPrincipal` application programming interfaces (APIs). To ensure compatibility with the default implementation for the **securityName** value, call the public `String` `getUserSecurityName(String uniqueUserId)` `UserRegistry` method.

## Expected format examples

Table 8. Format examples for `securityName`. This table gives expected format examples.

| User Registry | Format (securityName) value |
|---------------|-----------------------------|
| LDAP          | kevin                       |
| Basic         | kevin                       |

The `com.ibm.wsspi.security.cred.securityname` property is required.

- `com.ibm.wsspi.security.cred.group`

### Reference to the property

`AttributeNameConstants.WSCREDENTIAL_GROUP`

### Returns

`java.util.ArrayList`

### Explanation

This key searches for the array list of groups to which the user belongs. The groups are specified in the `realm_name/user_name` format. The format of these groups is important because the groups are used by the Liberty authorization engine for group-to-role mappings in the deployment descriptor. The format that is provided must match the format expected by the Liberty default implementation. When you use a third-party authorization provider, you must use the format that is expected by the third-party provider. To ensure compatibility with the default implementation for the unique group IDs value, call the public `List` `getUniqueGroupIds(String uniqueUserId)` `UserRegistry` method.

## Expected format examples

Table 9. Format examples for `group`. This table gives some format examples when configuring inbound identity mapping.

| User Registry | Format (group) value                      |
|---------------|-------------------------------------------|
| LDAP          | ldapRegistryRealm/cn=group1,o=Groups,c=US |
| Basic         | basicRegistryRealm/group1                 |

The `com.ibm.wsspi.security.cred.group` property is required. A user is not required to be associated groups.

- `com.ibm.wsspi.security.cred.cacheKey`

#### Reference to the property

`AttributeNameConstants.WSCREDENTIAL_CACHE_KEY`

#### Returns

`java.lang.Object`

#### Explanation

This key property can specify an object that represents the unique properties of the login, including the user-specific information and the user dynamic attributes that might affect uniqueness. For example, when the user logs in from location A, which might affect their access control, the cache key must include location A so that the received Subject is the correct Subject for the current location.

This `com.ibm.wsspi.security.cred.cacheKey` property is not required. When this property is not specified, the cache lookup is the value that is specified for `WSCREDENTIAL_UNIQUEID`. When this information is found in the `java.util.Hashtable` object, Liberty creates a Subject similar to the Subject that goes through the normal login process, at least for LTPA. The new Subject contains a `WSCredential` object and a `WSPrincipal` object that is fully populated with the information found in the `Hashtable` object.

## Single sign-on for HTTP requests using SPNEGO web authentication



8.5.5.5

You can securely negotiate and authenticate HTTP requests for protected resources in the WebSphere Application Server by using the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) as the web authentication service for WebSphere Application Server.

The following sections describe SPNEGO web authentication in more detail:

- “What is SPNEGO?”
- “SPNEGO web authentication in a single Kerberos realm” on page 988
- “SPNEGO web authentication in trusted Kerberos realms” on page 989
- “Support information for SPNEGO web authentication with a browser client” on page 991

### What is SPNEGO?

SPNEGO is a standard specification that is defined in The Simple and Protected GSS-API Negotiation Mechanism (IETF RFC 2478).

When Liberty server security is enabled, and SPNEGO web authentication is enabled, SPNEGO is initialized when processing a first inbound HTTP request. When the authentication filter is not specified, or the authentication filter is specified and the criteria is met, SPNEGO is responsible for authenticating access to the protected resource that is identified in the HTTP request.

In addition to WebSphere Application Server security runtime services, some external components are required to enable the operation of SPNEGO. These external components include:

-  Microsoft Windows Servers with Active Directory domain and associated Kerberos Key Distribution Center (KDC).
- A client application, for example, Microsoft .NET, or web service and J2EE client that supports the SPNEGO web authentication mechanism, as defined in IETF RFC 2478. Microsoft Internet Explorer and Mozilla Firefox are browser examples. Any browser that is being used must be configured to use the SPNEGO web authentication mechanism.

The authentication of HTTP requests is triggered by the user (the client-side), which generates an SPNEGO token. WebSphere Application Server receives this token. Specifically, the SPNEGO web authentication decodes and retrieves the user identity from the SPNEGO token. The identity is then used to make authorization decisions.

SPNEGO web authentication is a server-side solution in the WebSphere Application Server. Client-side applications are responsible for generating the SPNEGO token for use by SPNEGO web authentication. The user identity in the WebSphere Application Server security registry must be identical to the identity that the SPNEGO web authentication retrieves. An identical match does occur when Microsoft Windows Active Directory server is the Lightweight Directory Access Protocol (LDAP) server that is used in WebSphere Application Server. A custom login module is available as a plug-in to support custom mapping of the identity from the Active Directory to the WebSphere Application Server security registry.

WebSphere Application Server validates the identity against its security registry. If the validation is successful, the client GSS delegation credential is retrieved and placed in the client subject, and a Lightweight Third Party Authentication (LTPA) security token is created. It then returns the LTPA cookie to the user in the HTTP response. Subsequent HTTP requests from this same user to access more protected resources in the WebSphere Application Server use the LTPA security token that is previously created to avoid repeated login challenges.

### SPNEGO web authentication in a single Kerberos realm

SPNEGO web authentication is supported in a single Kerberos realm (domain). The challenge-response handshake process is shown in the following figure:

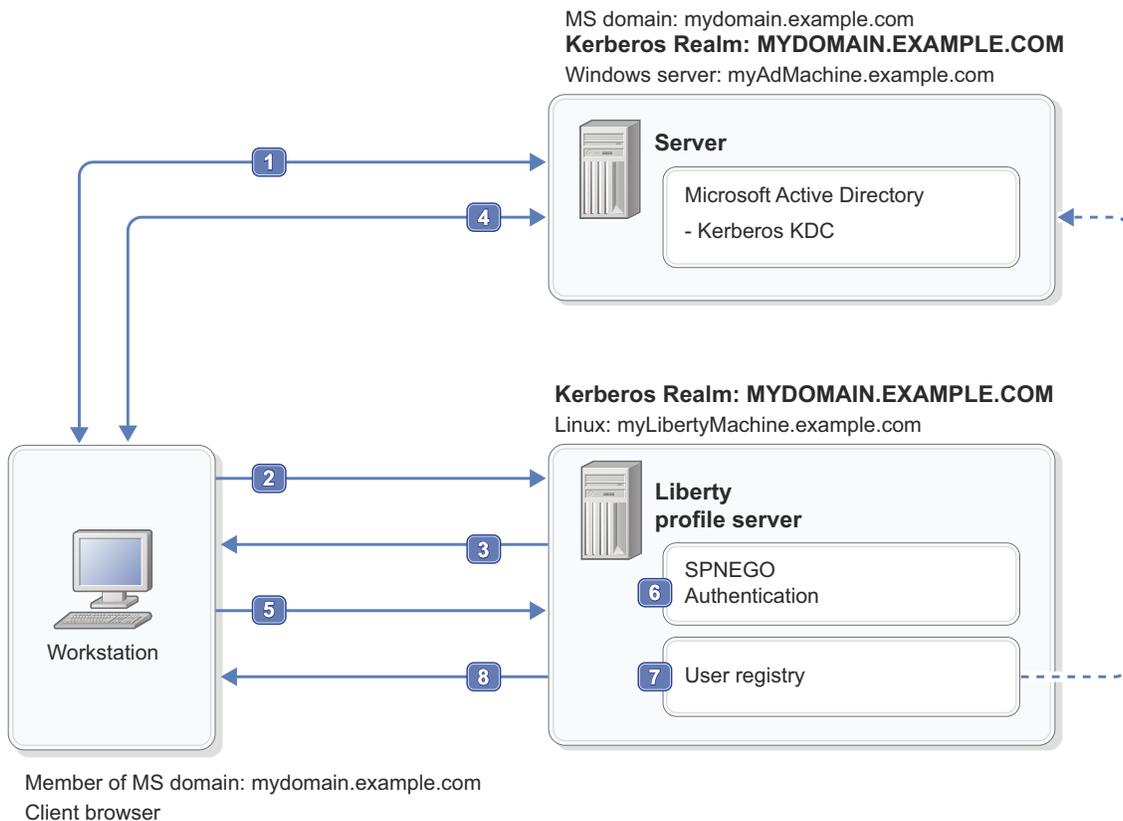


Figure 8. SPNEGO web authentication in a single Kerberos realm

In the previous figure, the following events occur:

1. To begin, the user logs on to the Microsoft domain controller MYDOMAIN.EXAMPLE.COM from the workstation.
2. Next, the user attempts to access the Web application. The user requests a protected Web resource using a client browser, which sends an HTTP GET request to the Liberty server.
3. SPNEGO authentication in the Liberty server answers the client browser with an HTTP 401 challenge header that contains the Authenticate: Negotiate status.
4. The client browser recognizes the negotiate header because the client browser is configured to support integrated Windows authentication. The client parses the requested URL for the host name. The client uses the host name to form the target Kerberos service principal name (SPN) HTTP/myLibertyMachine.example.com to request a Kerberos service ticket from the Kerberos ticket-granting service (TGS) in the Microsoft Kerberos KDC (TGS\_REQ). The TGS then issues a Kerberos service ticket (TGS\_REP) to the client. The Kerberos service ticket (SPNEGO token) proves both the user's identity and permissions to the service (Liberty server).
5. The client browser then responds to the Liberty server Authenticate: Negotiate challenge with the SPNEGO token that is obtained in the previous step in the request HTTP header.
6. SPNEGO authentication in the Liberty server sees the HTTP header with the SPNEGO token, validates the SPNEGO token, and gets the identity (principal) of the user.
7. After the Liberty server gets the identity of the user, it validates the user in its user registry and performs the authorization checks.
8. If access is granted, the Liberty server sends the response with an HTTP 200. The Liberty server also includes an LTPA cookie in the response. This LTPA cookie is used for subsequent requests.

**Note:** Other clients (for example, web services, .NET and J2EE) that support SPNEGO do not have to follow the challenge-response handshake process as shown previously. Those clients can obtain a ticket-granting ticket (TGT) and a Kerberos service ticket for the target server, create an SPNEGO token, insert it in the HTTP header, and then follow the normal process for creating an HTTP request.

### **SPNEGO web authentication in trusted Kerberos realms**

SPNEGO web authentication is also supported in trusted Kerberos realms. The challenge-response handshake process is shown in the following figure:

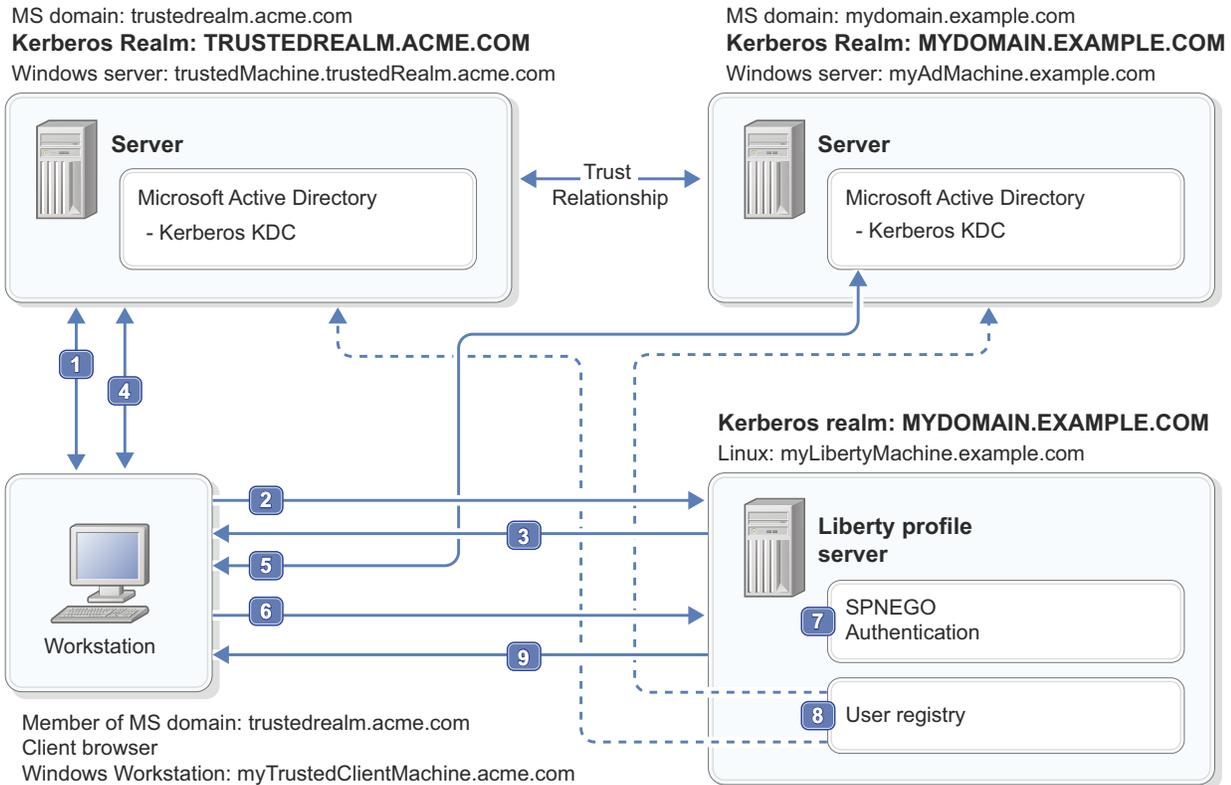


Figure 9. SPNEGO web authentication in a trusted Kerberos realm

In the previous figure, the following events occur:

1. The user logs in to the Microsoft domain controller TRUSTEDREALM.ACME.COM.
2. From a client browser, the user makes a request for a protected Web resource that is hosted on a Liberty server in the original Microsoft domain controller, MYDOMAIN.EXAMPLE.COM.
3. The Liberty server answers the client browser with an HTTP 401 challenge header that contains the `Authenticate: Negotiate` status.
4. The client browser is configured to support integrated Windows authentication. The client browser parses the URL by using the host name of the workstation that hosts the Liberty server application. The client browser uses the host name as an attribute to request a Kerberos cross-realm ticket (TGS\_REQ) for MYDOMAIN.EXAMPLE.COM from realm TRUSTEDREALM.ACME.COM.
5. The client browser uses the Kerberos cross-realm ticket from step 4 to request a Kerberos service ticket from realm MYDOMAIN.EXAMPLE.COM. The Kerberos service ticket (SPNEGO token) proves the user's identity and permissions to the service (Liberty server).
6. The client browser then responds to the Liberty server `Authenticate: Negotiate` challenge with the SPNEGO token that is obtained in the previous step in the request HTTP header.
7. The Liberty server receives the request and checks the HTTP header with the SPNEGO token. It then extracts the Kerberos service ticket, validates the ticket, and gets the identity (principal) of the user.
8. After the Liberty server gets the identity of the user, it validates the user in its user registry and performs the authorization checks.
9. If access is granted, the Liberty server sends the response with an HTTP 200. The Liberty server also includes an LTPA cookie in the response. This LTPA cookie is used for subsequent requests.

**Note:** No modification is required to the Liberty server to support more trusted realms. A trust relationship between the necessary Active Directory realms is the only requirement for SPNEGO to work with trusted realms.

In the trusted Kerberos realms environment, be aware that the Kerberos trusted realm setup has to be completed on each of the Kerberos KDCs. See your Kerberos Administrator and User's guide for more information about how to set up Kerberos trusted realms.

## Support information for SPNEGO web authentication with a browser client

The following scenarios are supported:

- Cross-forest trusts
- Domain trust within the same forest
- Kerberos realm trust

The following scenarios are not supported:

- Forest external trusts
- Domain external trusts

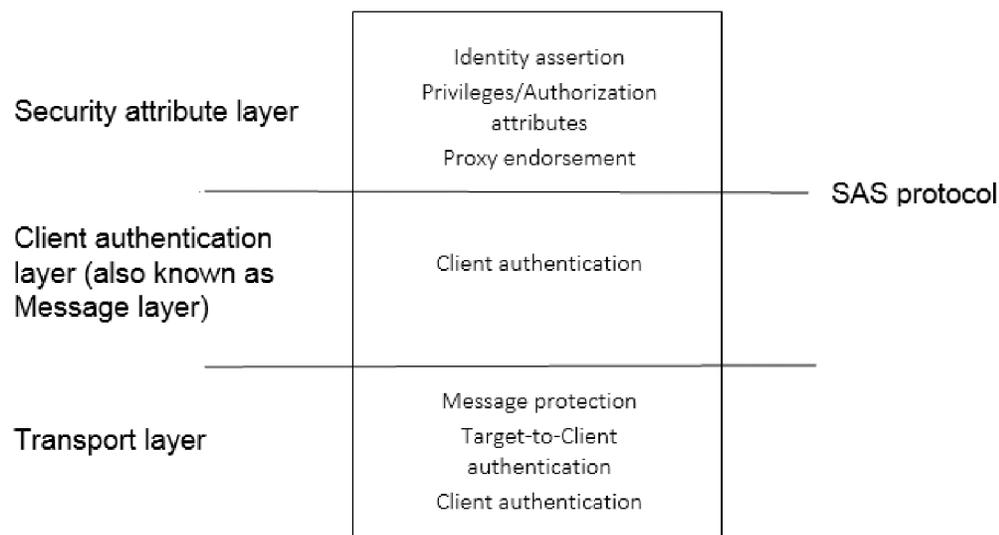
For further information on configuring SPNEGO on the Liberty server, see  [8.5.5.5](#) Configuring SPNEGO authentication in Liberty.

## Common Secure Interoperability version 2 (CSIv2)

8.5.5.6

The Common Secure Interoperability version 2 (CSIv2) is an architecture to satisfy the CORBA security interoperability requirements for authentication, delegation, and privileges. The SAS protocol is used in the CSIv2 architecture to exchange tokens in the service contexts of GIOP request and reply messages for the establishment of security contexts. Transport layer security (SSL/TLS) is required by SAS, and it provides two more layers on top for client authentication and delegation.

The SAS protocol is divided into two layers. The authentication layer is used to perform client authentication where sufficient authentication might not be accomplished in the transport. The attribute layer might be used by a client to push or deliver security attributes, like an identity to a target server where they might be applied in access control decisions. The transport is referred to as another layer in the CSIv2 documentation for ease of discussion, although it is not part of the SAS protocol message and the SAS message sits on top of the transport.



## CSIV2 identity assertion

The CSIV2 identity assertion support in the attribute layer is used to assert an identity from a client process to a server process when the request is performed by using RMI/IIOP.

An assertion is a declaration of one entity to another to accept an identity on its behalf. A client can assert an identity that represents the subject that was effective at the time it started the remote resource. In addition to the identity token that is representing the user, the client process also sends its own identity in either the authentication layer or the transport layer. The target server ensures that the client process is able to assert an identity by performing a trust validation. If the target server trusts the client, then the server uses the asserted identity to create a server-side subject that represents the user that was effective at the client process at the time of invocation.

The client can assert a user who is using a Principal Name identity token. The format of the principal name depends on the user registry that is configured at the client process. The anonymous identity token type is also supported and the server uses the unauthenticated subject when it receives such token.

For information on configuring the CSIV2 attribute layer with identity assertion, see “Configuring inbound CSIV2 attribute layer” on page 1974 or “Configuring outbound CSIV2 attribute layer” on page 1979.

## CSIV2 authentication layer

The CSIV2 authentication layer is used to carry authentication information from a client process to a server process when the request is performed by using RMI/IIOP.

The CSIV2 authentication layer can contain a token that is sent by the client that the server can then use to authenticate the client. Various token types are supported in the authentication layer. For example, the GSSUP token is used to transmit the client's user name and password, which is validated against the user registry of the target server. The Lightweight Third Party Authentication (LTPA) token is a token that represents the client's user without having to transmit a password, but the user must be authenticated at the client process before the remote method invocation and both the client and server processes must share LTPA keys.

With either token type, the token is used to authenticate the remote user at the server process and create a Subject representation of the Subject that was effective at the client side before the client started the remote object. When identity assertion is also enabled, the authentication layer can contain the security information that represents the client identity while the identity assertion token represents the actual remote user at invocation time.

For information on configuring the CSIV2 authentication layer, see “Configuring inbound CSIV2 authentication layer” on page 1976 or “Configuring outbound CSIV2 authentication layer” on page 1981.

## CSIV2 transport layer

The Common Secure Interoperability version 2 (CSIV2) transport layer support is used to protect the SAS protocol request message and support client certificate authentication from a client process to a server process.

The main function of the transport layer is to provide the security characteristics of the transmission of the SAS protocol messages from a client to a server process. The messages can be protected by using encryption, signing, or both. The Liberty SSL support is used as the underlying mechanism that is providing such characteristics.

A second function of the transport layer is to provide a source of authentication material when the authentication layer is not used. If identity assertion is enabled and the authentication layer is not

enabled, then the client process identity is obtained from the transport's client certificate chain. The target server process authenticates the client's certificate chain by mapping it to a user in its user registry. The certificate chain issuer distinguished name is used to determine if the client is trusted to assert an identity.

If no identity assertion and authentication layer are enabled, the subject that is obtained from mapping the client certificate chain is used as the caller subject when the actual remote method call is started at the target server process. This also applies when the target server's authentication layer is supported, but not required, and the client did not send an authentication token and an identity token.

For information on configuring the CSIV2 attribute layer with identity assertion, see [Configuring inbound CSIV2 transport layer](#) or [Configuring outbound CSIV2 transport layer](#).

## Key terms

### ORB – Object Request Broker.

It mediates object method invocations among entities, which might or might not be collocated in the same process.

### Security context

Information that is used to prescribe what the security characteristics are for a particular operation on an object in an ORB. For example, the identity that is to be used during the invocation of the object operation.

### Client security service or CSS

The entity that is initiating a SAS protocol request to establish a security context in the Target Security Service for an operation on an object in the target's ORB.

### Target security service or TSS

The entity that is receiving a SAS protocol request for the establishment of a security context in relationship to an operation on an object in its ORB. It accepts or denies a request to establish or use a security context.

### Client authentication

A token-based mechanism that is used to authenticate the client. GSSUP (Username Password GSS) is the minimum requirement, but there might be others, like LTPA.

### Identity assertion

Mechanism by which an intermediary entity vouches for another entity and the TSS uses the asserted identity for the invocation principal. The TSS can decide whether it trusts the proxy that is asserting the identity or not.

### Stateless

The security context is only used during the duration of a single request and it is not reused for subsequent requests.

### Stateful

The security context can be reused by multiple requests after it is established and until it is invalidated by the TSS or the CSS.

### Transport layer security

The security support that is provided by the underlying transport.

## Authentication on the Liberty application client container



8.5.5.6

The authentication requirements on the client are the same as on the server, but some of the mechanisms to authenticate on the client are different than on the server.

Authentication is required on the client when accessing a protected resource on the server. Follow one of these methods to provide the authentication information:

- Specify a user and password in the `client.xml` file: The credentials are sent to the server using the CSIV2 protocol and it is recommended that you encrypt or encode the password. For further details, see [Configuring the outbound CSIV2 authentication layer in the Liberty application client container](#).

- **Client certificate authentication:** The client presents the server a certificate, which is authenticated and mapped to a user in the registry for authorization checks. To configure the server, see [Configuring inbound CSIV2 transport layer](#). To configure the client, see [Configuring the outbound CSIV2 transport layer in the Liberty application client container](#).
- **Perform a programmatic login:** Programmatic login is a type of form login that supports application presentation login forms for authentication. This approach requires the application developer to collect the user's credentials and authenticate that user. For further details, see [Configuring a JAAS programmatic login on the Liberty application client container](#).

As on the server, you can use a custom login module to either make more authentication decisions or add information to the subject to make finer-grained authorization decisions inside your client application. For further details, see [Configuring a JAAS custom login module for the Liberty application client container](#).

## SAML 2.0 Web Browser Single-Sign-On



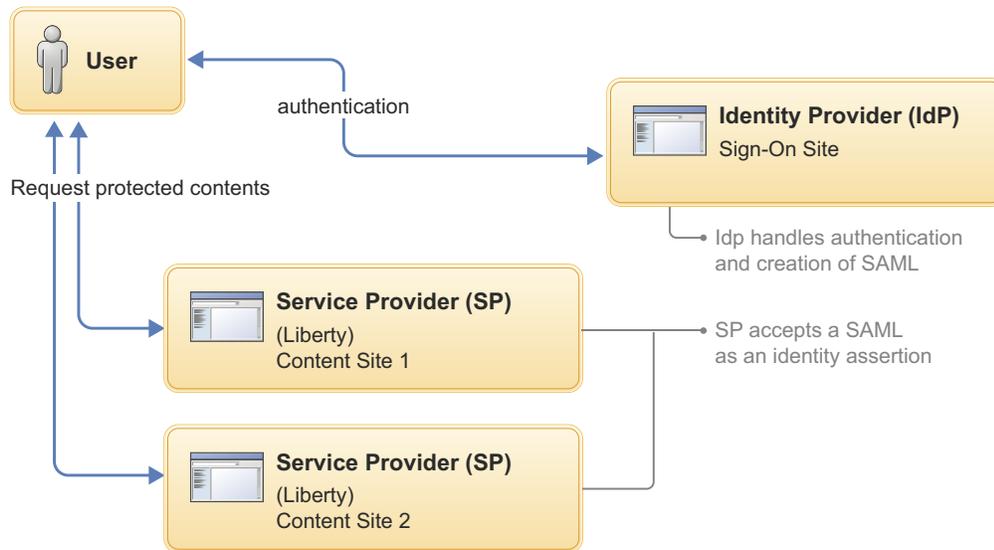
8.5.5.7

SAML Web Browser Single-Sign-On (SSO) enables web applications to delegate user authentication to a SAML identity provider instead of a configured user registry.

Security Assertion Markup Language (SAML) is an OASIS open standard for representing and exchanging user identity, authentication, and attribute information. A SAML assertion is an XML formatted token that is used to transfer user identity and attribute information from the identity provider of a user to a trusted service provider as part of the completion of a single sign-on request. A SAML assertion provides a vendor neutral means of transferring information between federation business partners. Using SAML, an enterprise service provider can contact a separate enterprise identity provider to authenticate users who are trying to access secure content.

The WebSphere Application Server Liberty supports the SAML web browser single sign-on profile with HTTP Post bindings, and acts as a SAML service provider. A web user authenticates to a SAML identity provider, which produces a SAML assertion, and the WebSphere SAML service provider uses the SAML assertion to establish a security context for the web user.

The SAML web SSO flow includes three actors: the end user, the identity provider (IdP), and the service provider (SP). The user always authenticates to the IdP, and the SP relies on IdP assertion to identify the user.

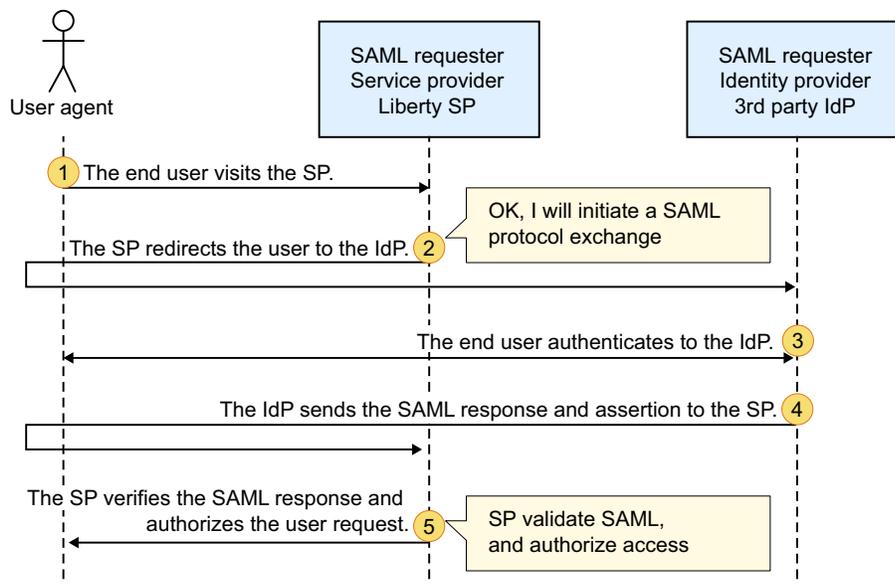


1. User requests a service from SP.
2. SP requests a user identity (SAML) from the IdP via redirect.
3. IdP asks user to login  
(There is no sign-in if user has been authenticated).
4. SP obtains SAML
5. SP makes an access control decision on the basis of SAML assertion

Figure 10. Key Concepts in Web Single-Sign-On

## Liberty SAML Web Browser SSO Scenarios

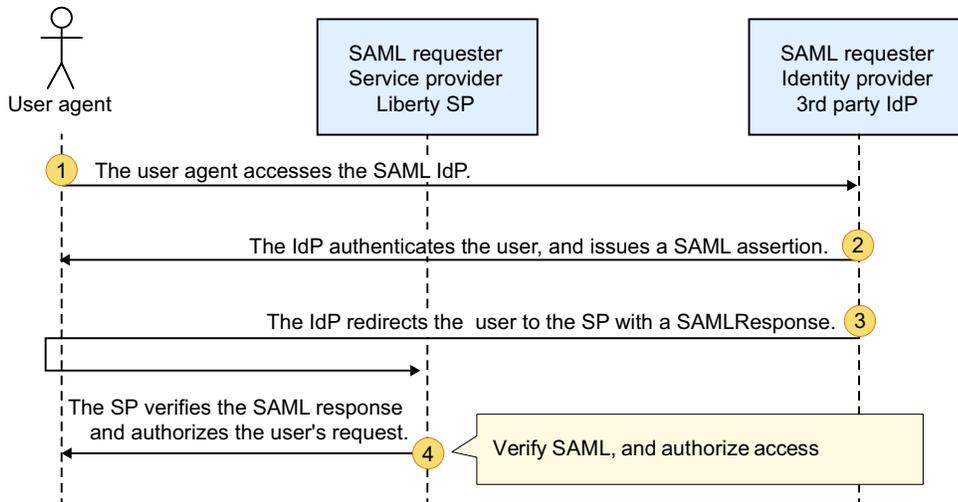
Figure 11. Scenario 1: SP-Initiated solicited Web SSO (End user starting at SP)



1. The end user visits the SP.
2. The SP redirects the user to the IdP.
3. The end user authenticates to the IdP.

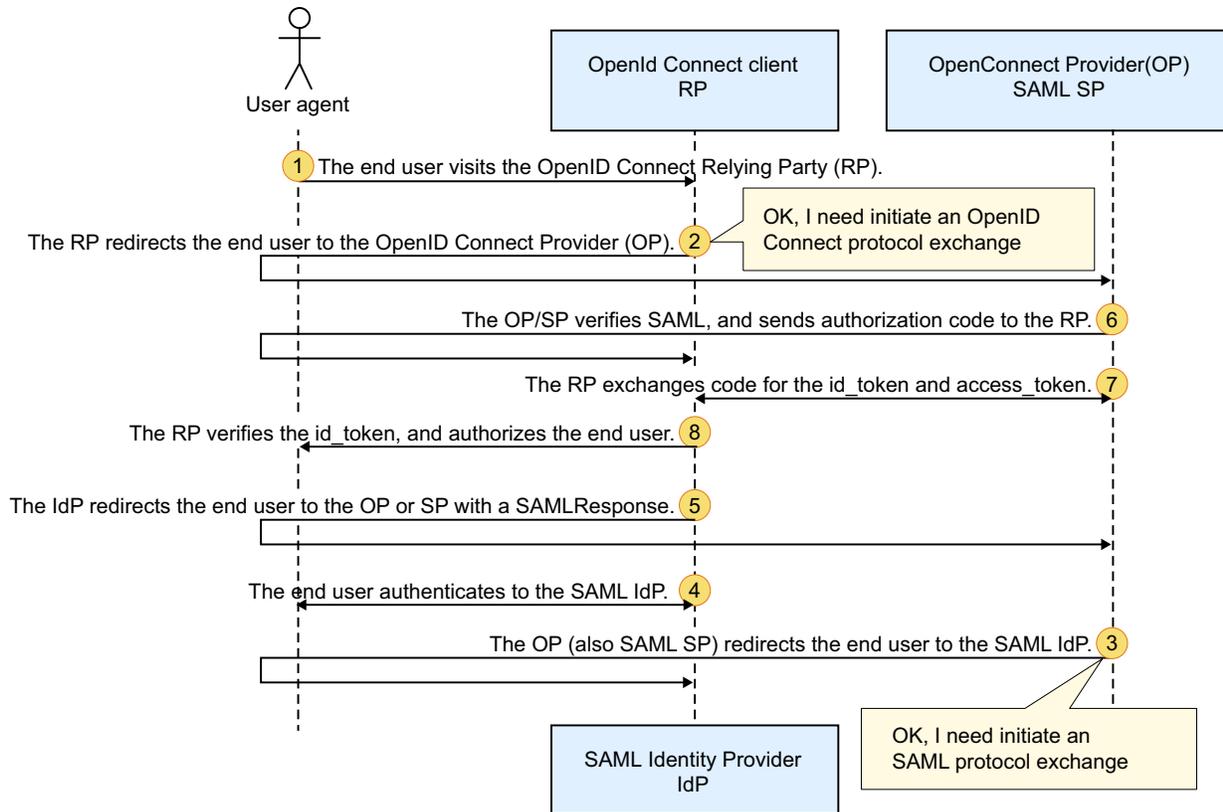
4. The IdP sends the SAML response and assertion to the SP.
5. The SP verifies the SAML response and authorizes the user request.

Figure 12. Scenario 2: IdP-Initiated unsolicited Web SSO (End user starting at IdP)



1. The user agent accesses the SAML IdP.
2. The IdP authenticates the user, and issues a SAML assertion.
3. The IdP redirects the user to the SP with a SAMLResponse
4. The SP verifies the SAML response and authorizes the user's request.

Figure 13. Scenario 3: OpenID Connect provider and SAML service provider



1. The end user visits the OpenID Connect Relying Party (RP).
2. The RP redirects the end user to the OpenID Connect Provider (OP).
3. The OP (also SAML SP) redirects the end user to the SAML IdP.
4. The end user authenticates to the SAML IdP.
5. The IdP redirects the end user to the OP or SP with a SAMLResponse.
6. The OP/SP verifies SAML, and sends authorization code to the RP.
7. The RP exchanges code for the id\_token and access\_token.
8. The RP verifies the id\_token, and authorizes the end user.

## Federation of user registries

8.5.5.8

User registry federation is used when user and group information is spread across multiple registries. For example, the information might be in two different LDAPs, in two subtrees of the same LDAP, in a file, or the users are of a system. The information might even be in a custom user data repository. With registries federated, you can search and use these distributed user information in a unified manner with continuous store of information. Using federated registry, you can use the unified view for authentication and authorization of users in Liberty.

**Note:** Quick start security (quickStartSecurity) cannot be federated with other user registries such as the LDAP, basic, SAF, and custom registries.

### How are user registries federated?

LDAP registries are federated by default. If more than one LDAP registry is configured in the server.xml, then the registries are automatically federated and no additional configuration is needed. They can be two separate LDAPs or two subtrees in the same LDAP.

If one or more LDAP registries are configured with one or more of basic, SAF, or custom registries, those registries are also federated without any additional configuration. The following example shows a basic registry federated with an LDAP:

```
<server description="Federation">
  <featureManager>
    <feature>appSecurity-2.0</feature>
    <feature>servlet-3.0</feature>
  <feature>ldapRegistry-3.0</feature>
  </featureManager>

  <basicRegistry id="basic" realm="SampleBasicRealm">
    <user name="admin" password="password" />
    <user name="user1" password="password" />
    <user name="user2" password="password" />
    <group name="memberlessGroup" />
    <group name="adminGroup">
      <member name="admin"/>
    </group>
    <group name="users">
      <member name="user1"/>
      <member name="user2"/>
    </group>
  </basicRegistry>

  <ldapRegistry id="LDAP1" realm="SampleLdapIDSRealm" host="LDAPHOST1.ibm.com" port="389" ignoreCase="true"
baseDN="o=ibm,c=us"
ldapType="IBM Tivoli Directory Server"
searchTimeout="8m"
recursiveSearch="true">
  </ldapRegistry>
</server>
```

If you want to federate two basic registries or a basic registry with a SAF or custom registry, you can do so by including the federatedRegistry-1.0 in addition to the appSecurity-2.0 feature as shown in the following example.

```
<feature>appSecurity-2.0</feature>
<feature>federatedRegistry-1.0</feature>
```

The following example shows the federation of two basic registries:

```
<server description="Federation">
  <featureManager>
    <feature>appSecurity-2.0</feature>
    <feature>federatedRegistry-1.0</feature>
  </featureManager>

  <basicRegistry id="basic1" realm="SampleBasicRealm1">
    <user name="admin" password="password" />
    <user name="user1" password="password" />
    <user name="user2" password="password" />
    <group name="memberlessGroup" />
    <group name="adminGroup">
      <member name="admin"/>
    </group>
    <group name="users">
      <member name="user1"/>
      <member name="user2"/>
    </group>
  </basicRegistry>

  <basicRegistry id="basic2" realm="SampleBasicRealm2">
    <user name="user3" password="password123" />
    <user name="user4" password="password123" />
    <group name="memberlessGroup2" />
    <group name="users2">
      <member name="user3"/>
    </group>
  </basicRegistry>
</server>
```

```
        <member name="user4"/>
    </group>
</basicRegistry>
</server>
```

## Liberty: Authorization

Authorization in Liberty determines whether a user has access to a certain role within the system.

Authorization specifies access rights to resources. It usually follows authentication that confirms an identity. Whereas authentication answers the question: “Are you who you say you are?”; authorization answers the question: “Do you have permission to do what you are trying to do?”

The following sections describe these concepts in detail:

- “Authorization for administrative functions”
- “Authorization for applications”
- “Special subjects” on page 1000
- “Access IDs and authorization” on page 1001

### Authorization for administrative functions

When an entity attempts to access a resource, the authorization service determines whether that entity has the required rights to access the resource. This concept holds true whether an entity is accessing an application or performing administrative functions. The main difference between authorizing access to an application and access to an administrative function lies in how the users are mapped to roles. For authorization of applications, use the `application-bnd` element in the `server.xml` file or the `ibm-application-bnd.xml/xmi` file to map the users to roles. For authorization of administrative functions, use the `administrator-role` element in the `server.xml` file to map the users to the administrator role. For more information about administrative security, see “Connecting to Liberty by using JMX” on page 1641.

### Authorization for applications

The following diagram describes how authorization works for applications:

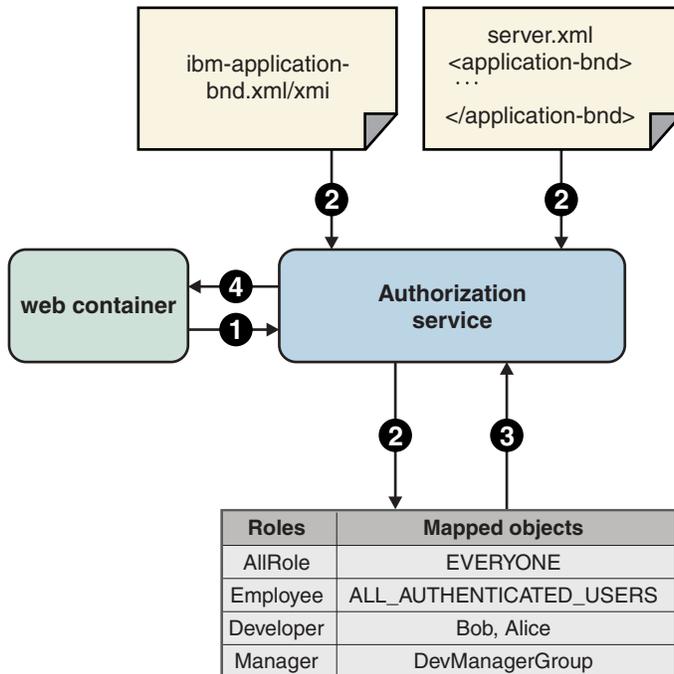


Figure 14. Overview of authorization process

1. An authorization is made when an entity attempts to access a resource in an application that is served by Liberty. The web container calls the authorization service to determine whether a user has permission to access a certain resource, given a set of one or more required roles. The required roles are determined by the `auth-constraint` elements in the deployment descriptor and `@ServletSecurity` annotations.
2. The authorization service determines what objects the required role is mapped to. This step is accomplished by processing the mappings that are defined in the `ibm-application-bnd.xmi` file or the `ibm-application-bnd.xml` file, and the `application-bnd` element of the `server.xml` file. The mappings from these two sources are merged. If the same role is present in both sources, only the role mapping in the `server.xml` file is used. The advantage of using the `server.xml` file for mapping roles to users is that your application does not need to be packaged into an EAR file and it is easier to update. Alternatively, using the `ibm-application-bnd.xmi/xml` file makes your application portable to other servers and other traditional servers that do not support the `server.xml` file.
3. If the required role is mapped to the **EVERYONE** special subject, then the authorization service returns immediately to allow anyone access. If the role is mapped to the **ALL\_AUTHENTICATED\_USERS** special subject and the user is authenticated, then the authorization service grants access to the user. If none of these conditions are met, then the authorization service determines what users and groups are mapped to the required role. The authorization service grants access to the resource if the user is mapped to the required role or if the user is part of a group that is mapped to the role.
4. The authorization service returns a result back to the web container to indicate whether the user is granted or denied access.

## Special subjects

When you map entities to roles, you can map a special subject instead of a specific user or group. A special subject is an extension to the concept of a subject. A special subject can represent a group of users that fall under a specific category.

The following two types of special subjects are available:

- **EVERYONE**: represents any entity on the system, which means that no security is available because everyone is allowed access and you are not prompted to enter credentials.

- ALL\_AUTHENTICATED\_USERS: represents any entity that successfully authenticates to the server.

To map a special subject to a user, update either the `ibm-application-bnd.xml/xmi` file or the `server.xml` file, where the `application-bnd` is under the `application` element. In this example, the role that is named `AllAuthenticated` is mapped to the special subject `ALL_AUTHENTICATED_USERS`:

```
<application-bnd>
  <security-role name="AllAuthenticated">
    <special-subject type="ALL_AUTHENTICATED_USERS" />
  </security-role>
</application-bnd>
```

See “Configuring authorization for applications in Liberty” on page 1939.

## Access IDs and authorization

When you authorize a user or group, the server needs a way to uniquely identify that user or group. The unique ID of the user and group serve this purpose and are used to build the authorization configuration. These IDs are determined by the user registry implementation: the unique user ID is the value of `getUniqueUserId()`, and the unique group ID is the value of `getUniqueGroupId()`. You can also choose to explicitly specify an access ID for the user or group in the authorization configuration. These explicit access IDs are used instead of the values that are returned by the user registry implementation. To specify an access ID in the `ibm-application-bnd.xml/xmi` file or the `server.xml` file, where the `application-bnd` is under the `application` element, use the **access-id** attribute for the user or group element.

In this example, an access ID is specified for the user `Bob` and the group `developers`:

```
<application-bnd>
  <security-role name="Employee">
    <user name="Bob" access-id="user:MyRealm/Bob"/>
    <group name="developers" access-id="group:myRealm/developers"/>
  </security-role>
</application-bnd>
```

**Note:** The **access-id** attribute is used for the authorization check. If it is not specified, it is determined from the registry that is configured by using the user or group name. However, you must specify the **access-id** attribute as shown in the example when the users or groups do not belong to the active registry. Such as when you are using a programmatic login.

## Security on the Liberty application client container



8.5.5.6

Security on the Liberty application client container includes SSL, JAAS, and CSIV2.

Application clients are client programs that run in their own Java virtual machines. The Liberty application client container provides system services for these clients, including security. The security services on the client are a subset of those that are available on the server.

### Enabling security on the client

To enable security on the client, add the `appSecurityClient-1.0` feature to your `client.xml` file.

```
<featureManager>
  <feature>javaeeClient-7.0</feature>
  <feature>appSecurityClient-1.0</feature>
</featureManager>
```

The `appSecurityClient-1.0` feature enables SSL, CSiv2, and JAAS on the client. You must configure SSL to ensure communications between the client and server are secure and encrypted. For more information, see [Enabling SSL communication for the Liberty application client container](#). CSiv2 provides a protocol for the client to send authentication information to the server. The client in a Liberty application client container is not able to assert identities or propagate security attributes. To understand more about CSiv2 and how to configure it on the client, see [Common Secure Interoperability version 2 \(CSiv2\)](#), and [Configuring Common Secure Interoperability version 2 \(CSiv2\) in the Liberty application client container](#). The JAAS framework on the client enables a client application to gather credentials from the user that is using callbacks, and authenticate that user by using login modules. For more information about authenticating users on the client, see [“Authentication on the Liberty application client container”](#) on page 993.

## Liberty: Java 2 Security

8.5.5.7

Java 2 Security functionality is supported in WebSphere Application Server Liberty. Java 2 Security provides a policy-based, fine-grained access control mechanism that increases overall system integrity by checking for permissions before allowing access to certain protected system resources.

Java 2 Security is independent of Java Platform, Enterprise Edition role-based authorization. Java 2 Security guards access to system resources such as file input and output, sockets, and properties; whereas Java Platform, Enterprise Edition security guards access to web resources such as servlets and JSP files.

### Java 2 Security for deployers and administrators

Before you enable Java 2 Security, you need to make sure that all the applications are granted the required permissions, otherwise, applications might fail to run. By default, applications are granted the permissions per the Java Platform, Enterprise Edition 7.0 specification. If an application is not prepared for Java 2 Security or if the application provider does not provide a `permissions.xml` file as part of the application, then the application might cause Java 2 Security access control exceptions at run time when Java 2 Security is enabled. Even if the application is running, it might not run correctly.

### Java 2 Security for application developers

Application developers must understand the permissions that are granted in the default WebSphere policy and the permission requirements of the Java SDK APIs. You need to know whether the APIs that your application calls require extra permissions or not. For more information about which Java APIs require permissions, see [Permissions in the Java 2 SDK](#).

Permissions are added to an application by way of the `permissions.xml` file, and the codebase that is associated with the listed permissions is based on the location of the file. For a stand-alone `.war` application, the `permissions.xml` file is bundled under the `META-INF` directory and all specified permissions apply to all modules included in the `.war` file. For a `.ear` application, the `permissions.xml` is bundled directly under the `META-INF` directory for the `.ear` itself, and the specified permissions apply to all modules included in the `.ear` file.

**Note:** In the case of an `.ear` application, `permissions.xml` files that are bundled under the `META-INF` directory of any module other than the `.ear` are ignored.

### Enabling Java 2 Security

Java 2 Security functions are part of the kernel extension and are enabled at bootstrap time by updating the `bootstrap.properties` file with the `websphere.java.security` property.

If the `websphere.java.security` property is specified in the `bootstrap.properties` file, Java 2 Security is enforced; otherwise, no permission checking occurs.

## Specifying restricted permissions

Liberty provides a mechanism to specify restricted permissions when it runs a web or EJB application component. A restricted permission ensures no instance of that permission is granted to a bundle or application. They provide a mechanism to prevent applications from granting themselves more permissions than what must be allowed, for example, the permission to exit VM.

Restricted permissions are specified in the `server.xml` and `client.xml` files. The following example shows how the `PropertyPermission` that is used to write the System property `os.name` is restricted. This syntax is identical in both the `server.xml` and `client.xml` files:

```
<javaPermission className="java.security.PropertyPermission" name="os.name" actions="write" restriction="true" />
```

## Granting permissions

OSGi bundles can self-regulate the permissions that are granted to the libraries/classes within the bundle through the `permissions.perm` file.

Applications can also self-regulate permissions that are granted through the `permissions.xml` file, or by specifying the permission grants in the `server.xml` and `client.xml` files.

## OSGi bundle permissions

The OSGi specification provides a mechanism to specify permissions for a bundle through the `permissions.perm` file in the `OSGI-INF` directory of the bundle. The mechanism allows fine-grained access control of permissions for the bundle.

The `permissions.perm` file specifies the maximum permissions that the bundles require.

**Important:** An empty `permissions.perm` file is not equivalent to no `permissions.perm` file. Make sure that you have a non-empty `permissions.perm` file if you want restricted permissions.

## Declaring permissions in the `server.xml` and `client.xml` for applications

Permissions without a specified codebase, which are defined in the `server.xml` and `client.xml` files apply to all applications on that Liberty server.

You can specify the permissions to be granted in the `server.xml` and `client.xml` files as given in the following example. In this example, the `PropertyPermission` that enables all System properties to be read is granted:

```
<javaPermission className="java.util.PropertyPermission" name="*" actions="read" />
```

You can specify the permissions to be restricted in the `server.xml` and `client.xml` files. The following example shows how the `PropertyPermission` that is used to write the System property `os.name` is restricted. This syntax is identical in both the `server.xml` and `client.xml` files:

```
<javaPermission className="java.security.PropertyPermission" name="os.name" actions="write" restriction="true" />
```

### Notes:

- A restricted permission has **restriction** set to *true*.
- If an application attempts to grant itself a permission that is defined as a restricted permission, the restricted permission takes precedence over the grant and disallows the grant.

## Declaring permissions in permissions.xml for applications

The permissions.xml file is a new file that is introduced by the Java EE7 specification. It is packaged under the META-INF directory for an application.

For applications packaged as a stand-alone .war file, the permissions that are specified at the META-INF/WAR level apply to all modules and libraries that are packaged within the .war file.

For applications that are packages in an .ear file, the declaration of permissions must be at the .ear file level. This permission set is applied to all modules and libraries that are packaged within the .ear file or within its contained modules. Any permissions.xml file within such packaged modules is ignored, regardless of whether a permissions.xml file is supplied for the .ear file itself.

For applications that are packaged in a .rar file, the declaration of permissions must be at the META-INF/RAR level.

## No-rethrow option

When Java 2 Security is enabled, the JDK Security Manager throws an java.security.AccessControl exception by default when a permission violation occurs. If the exception is not handled, it might cause a runtime failure. To help the developers when they are preparing their applications for Java 2 Security, a no-rethrow option is available. The no-rethrow option allows the AccessControl exception to be logged in the console.log and messages.log but does not cause the application to fail. The no-rethrow option is enabled by specifying websphere.java.security.norethrow=true in the bootstrap.properties file. The no-rethrow option is not enabled by default, hence you must enable this property by specifying it in the bootstrap.properties file.

**Note:** Because this property does not allow the Security Manager to throw the exception, the Security Manager technically does not enforce Java 2 Security. The no-rethrow property must not be used in a production environment.

## Dynamic updates

Dynamic updates to the permission files such as the permissions.perm, permissions.xml, server.xml, and client.xml are not supported. Updates to permissions require a Liberty server restart.

## Liberty:Security public APIs

Security public APIs in Liberty provide a way of extending the security infrastructure.

Liberty contains public APIs that you can use to implement security functions. The security public APIs in Liberty are a subset of the traditional security public APIs. The main classes are WSSecurityHelper, WSSubject, and RegistryHelper. These classes contain a subset of the methods that are available in the WebSphere Application Server traditional versions. There is also a new class WebSecurityHelper.

The following sections describe those main classes. There are also other classes such as UserRegistry, WSCredential, and other exception classes.

All the security public APIs supported by Liberty are in the Java API documentation. The Java API documentation for each Liberty server API is available in a separate .zip file in one of the javadoc subdirectories of the \${wlp.install.dir}/dev directory.

### WSSecurityHelper

This class contains only the methods isServerSecurityEnabled() and isGlobalSecurityEnabled(). These calls return true if appSecurity-2.0 or zosSecurity-1.0, among others, is enabled. Otherwise, the methods return false. These methods are carried over from the traditional WSSecurityHelper class for compatibility.

**Note:**

- There are no cells in Liberty, so there is no distinction in Liberty between global security and server security. Therefore, both methods return the same value.
- The method `revokeSSOCookies(javax.servlet.http.HttpServletRequest req, javax.servlet.http.HttpServletResponse res)` is not supported in Liberty. Instead, you can use the Servlet 3.0 logout function.
- The method `getLTPACookieFromSSOToken()` is renamed to a new public API class: `WebSecurityHelper`.

**WSSubject**

This class provides utility methods for querying and setting the security thread context. All methods from the traditional `WSSubject` are supported in Liberty.

**Note:** Java 2 Security is supported but not enabled by default in Liberty. So by default, the Java 2 security checks in `WSSubject` are not performed.

**RegistryHelper**

This class provides access to the `UserRegistry` object and trusted realm information. In Liberty, it contains the following subset of the traditional methods:

```
public static UserRegistry getUserRegistry(String realmName) throws WSSecurityException
public static List<String> getInboundTrustedRealms(String realmName) throws
WSSecurityException
public static boolean isRealmInboundTrusted(String inboundRealm, String localRealm)
```

**Note:** This method involves dynamic information that could change as OSGI dynamic services change. The values that are retrieved can become stale. The `UserRegistry` references should never be cached.

**WebSecurityHelper**

This class contains the renamed `getLTPACookieFromSSOToken()` method, which was moved from `WSSecurityHelper`:

```
public static Cookie getSSOCookieFromSSOToken() throws Exception
```

**Security public API code examples**

The following examples demonstrate how to use security public APIs in Liberty to do a programmatic login and operate on the Subject.

- Example 1: Create a Subject and use it for authorization
- Example 2: Create a Subject and make it as the current Subject on the thread
- Example 3: Get information of the current Subject on the thread

**Example 1: Create a Subject and use it for authorization**

This example demonstrates how to use `WSSecurityHelper`, `WSSubject`, and `UserRegistry` to do a programmatic login to create a Java Subject, then perform an action and use that Subject for any authorization that is required.

**Note:** The following code uses `WSSecurityHelper` to check if security is enabled before doing further security processing. This check is used extensively because of the modular nature of Liberty: If security is not enabled, then the security run time is not loaded. `WSSecurityHelper` is always loaded, even if security is not enabled.

```
import java.rmi.RemoteException;
import java.security.PrivilegedAction;

import javax.security.auth.Subject;
import javax.security.auth.callback.CallbackHandler;
```

```

import javax.security.auth.login.LoginContext;
import javax.security.auth.login.LoginException;

import com.ibm.websphere.security.CustomRegistryException;
import com.ibm.websphere.security.UserRegistry;
import com.ibm.websphere.security.WSSecurityException;
import com.ibm.websphere.security.WSSecurityHelper;
import com.ibm.websphere.security.auth.WSSubject;
import com.ibm.websphere.security.auth.callback.WSCallbackHandlerImpl;
import com.ibm.wsspi.security.registry.RegistryHelper;
public class myServlet {

    ...
    if (WSSecurityHelper.isServerSecurityEnabled()) {
        UserRegistry ur = null;
        try {
            ur = RegistryHelper.getUserRegistry(null);
        } catch (WSSecurityException e1) {
            // record some diagnostic info
            return;
        }
        String userid = "user1";
        String password = "user1password";
        try {
            if (ur.isValidUser(userid)) {
                // create a Subject, authenticating with
                // a userid and password
                CallbackHandler wscbh = new WSCallbackHandlerImpl(userid, password);
                LoginContext ctx;
                ctx = new LoginContext("WSLogin", wscbh);
                ctx.login();
                Subject subject = ctx.getSubject();
                // Perform an action using the Subject for
                // any required authorization
                WSSubject.doAs(subject, action);
            }
        } catch (CustomRegistryException e) {
            // record some diagnostic info
            return;
        } catch (RemoteException e) {
            // record some diagnostic info
            return;
        } catch (LoginException e) {
            // record some diagnostic info
            return;
        }
    }
    ...
    private final PrivilegedAction action = new PrivilegedAction() {
        @Override
        public Object run() {
            // do something useful here
            return null;
        }
    };
}

```

### Example 2: Create a Subject and make it the current Subject on the thread

The following example demonstrates how to use WSSecurityHelper and WSSubject to do a programmatic login to create a Java Subject. Make that Subject the current Subject on the thread, and then restore the original security thread context.

**Note:** The following code uses WSSecurityHelper to check if security is enabled before doing further security processing.

```

import javax.security.auth.Subject;
import javax.security.auth.callback.CallbackHandler;
import javax.security.auth.login.LoginContext;
import javax.security.auth.login.LoginException;

import com.ibm.websphere.security.WSSecurityException;
import com.ibm.websphere.security.WSSecurityHelper;
import com.ibm.websphere.security.auth.WSSubject;
import com.ibm.websphere.security.auth.callback.WSCallbackHandlerImpl;
...
if (WSSecurityHelper.isServerSecurityEnabled()) {
    CallbackHandler wscbh = new WSCallbackHandlerImpl("user1", "user1password");
    LoginContext ctx;
    try {
        // create a Subject, authenticating with
        // a userid and password
        ctx = new LoginContext("WSLogin", wscbh);
        ctx.login();
        Subject mySubject = ctx.getSubject();
        Subject oldSubject = null;
        try {
            // Save a ref to the current Subject on the thread
            oldSubject = WSSubject.getRunAsSubject();
            // Make mySubject the current Subject on the thread
            WSSubject.setRunAsSubject(mySubject);
            // Do something useful here. Any authorization
            // required will be performed using mySubject
        } catch (WSSecurityException e) {
            // record some diagnostic info
            return;
        } finally {
            // Put the original Subject back on the thread context
            if (oldSubject != null) {
                try {
                    WSSubject.setRunAsSubject(oldSubject);
                } catch (WSSecurityException e) {
                    // record some diagnostic info
                }
            }
        }
    } catch (LoginException e) {
        // record some diagnostic info
        return;
    }
}

```

### Example 3: Get information of the current Subject on the thread

The following example demonstrates how to use `WSSecurityHelper`, `WSSubject`, and `WSCredential` to get information about the current Subject on the thread.

**Note:** The following code uses `WSSecurityHelper` to check if security is enabled before doing further security processing.

```

import java.util.ArrayList;
import java.util.Iterator;
import java.util.Set;

import javax.security.auth.Subject;
import javax.security.auth.login.CredentialExpiredException;

import com.ibm.websphere.security.WSSecurityException;
import com.ibm.websphere.security.WSSecurityHelper;
import com.ibm.websphere.security.auth.CredentialDestroyedException;
import com.ibm.websphere.security.auth.WSSubject;
import com.ibm.websphere.security.cred.WSCredential;
...
if (WSSecurityHelper.isServerSecurityEnabled()) {
    // Get the caller's subject

```

```

Subject callerSubject;
try {
    callerSubject = WSSubject.getCallerSubject();
} catch (WSSecurityException e) {
    // record some diagnostic info
    return;
}
WSCredential wsCred = null;
Set<WSCredential> wsCredentials =
    callerSubject.getPublicCredentials(WSCredential.class);
Iterator<WSCredential> wsCredentialsIterator = wsCredentials.iterator();
if (wsCredentialsIterator.hasNext()) {
    wsCred = wsCredentialsIterator.next();
    try {
        // Print out the groups
        ArrayList<String> groups = wsCred.getGroupIds();
        for (String group : groups) {
            System.out.println("Group name: " + group);
        }
    } catch (CredentialExpiredException e) {
        // record some diagnostic info
        return;
    } catch (CredentialDestroyedException e) {
        // record some diagnostic info
        return;
    }
}
}
}
}

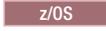
```

## Configuration differences between the traditional and Liberty: security

The configuration differences in the security capability between Liberty and traditional indicates the items that you might need to know during applications migration.

Liberty security supports only a subset of security features in the traditional. Unless the support is explicitly mentioned in Liberty documentation, you must assume that the support is not available yet.

The following security features are not included in Liberty:

- Not all public APIs and SPIs are supported. The Java API documentation for each Liberty API is available in a separate .zip file in one of the javadoc subdirectories of the `#{wlp.install.dir}/dev` directory.
- Horizontal propagation.
- SecurityAdmin MBean support, therefore methods such as clearing the authentication cache are not available.
- Java 2 Connector (J2C) principal mapping modules support.
- Multiple security domain support.
-   CSIV2 security attribute propagation.
-   Kerberos authentication.
-   SPNEGO on non-IBM JDK.
- Security auditing subsystem that is part of the security infrastructure of the server.
-  SAF delegation.
-  SAF authorization is not supported with a user registry that is not on the local operating system.
-  SAF distributed identity mapping.

In Liberty, you can configure user-to-role mappings and RunAs users in the `application-bnd` element of the `server.xml` file. **8.5.5.0** For a Run-As entry, the password is optional. In the traditional, you can only configure the Run-AS entry in the `ibm-application-bnd.xml/xmi` file. **8.5.5.0** For a Run-As entry, the password is required. See “Configuring authorization for applications in Liberty” on page 1939.

In Liberty, role names can be referenced by the `HttpServletRequest.isUserInRole` and `EJBContext.isCallerInRole` APIs or by elements in the deployment descriptor without first declaring the role names using the `@DeclareRoles` annotation or the `<security-role/>` element in the deployment descriptor. However, roles must be declared before being used in WebSphere Application Server traditional.

## Liberty: The limits to protection through password encryption

**8.5.5.0**

Liberty supports Advanced Encryption Standard (AES) encryption for passwords that are stored in the `server.xml` file. When you use this option for protecting system passwords in the Liberty configuration, you need to understand the limits to the protection it provides.

Encrypting a password in the Liberty configuration does not guarantee that the password is secure or protected; it only means that someone who can see the encrypted password, but does not know the encryption key, cannot easily recover the password. The application server process requires access to both the encrypted password and the decryption key, so both these data items need to be stored on the file system that is accessible to the server runtime environment. The encryption key is also required by anyone who encrypts a password that is placed in the server configuration. For an attacker that has access to exactly the same set of files as the Liberty server instance, applying AES encryption to the password therefore provides no additional security over and above “exclusive or” (XOR) encoding.

Nonetheless, there are still reasons why you might consider encrypting passwords in the Liberty configuration. The Liberty configuration is designed to be highly composable and sharable. The administration subsystem of traditional (the administrative console and `wsadmin` scripting) prevents an administrator from gaining access to an XOR-encoded password. Liberty is designed to be configured without an administration subsystem, and so any XOR-encoded password is visible to any administrator. Given these design features, consider the following scenarios:

- The passwords are not sensitive, so encoding them provides little value.
- The passwords are sensitive, so either the configuration files containing the password are security sensitive and access needs to be controlled, or the passwords are encrypted and the encoding key is then protected as security sensitive.

The encryption key used for decrypting can be overridden from the default by setting the `wlp.password.encryption.key` property. This property should not be set in the `server.xml` file that stores the password, but in a separate configuration file that is included by the `server.xml` file. This separate configuration file should contain only a single property declaration, and should be stored outside the normal configuration directory for the server. This ensures that the file containing the key is not included when you are running the `server dump` or `package` command. The encryption key property can also be specified as a bootstrap property. If you choose this option, you should put the encryption key in a separate properties file that is included in the `server bootstrap.properties` file.

For information about using XOR or AES to protect your passwords see the related links, especially “Liberty:securityUtility command” on page 1844.

---

## Liberty:JMS messaging

8.5.5.0

Liberty supports asynchronous messaging as a method of communication that is based on the Java Message Service (JMS) programming interface. The JMS interface provides a common way for Java programs (clients and Java EE applications) to create, send, receive, and read asynchronous requests as JMS messages. With Liberty, you can configure multiple JMS messaging providers, which can be used by the JMS applications.

The following JMS messaging providers are supported in Liberty:

- Liberty embedded messaging engine, as the JMS messaging provider
- Service integration bus, which is the default messaging provider of WebSphere Application Server traditional
- IBM MQ messaging provider, which uses the IBM MQ system as the provider

Your applications can use messaging resources from any of the three JMS providers. The choice of the provider is made based either on your messaging requirements or for integration with an existing messaging system. For example, you might want your applications to connect locally to the Liberty messaging provider without the need to configure any external messaging provider, in which case you would use the Liberty embedded messaging engine. Alternatively, you might want to integrate with your existing messaging infrastructure, such as IBM MQ. In such cases, you can either connect directly by using the IBM MQ messaging provider or configure a service integration bus with links to the IBM MQ network and then access the bus through the default messaging provider.

### Liberty JMS messaging providers



8.5.5.6

Different JMS messaging providers are supported in Liberty.

#### Liberty embedded JMS messaging provider



8.5.5.6

Liberty messaging is an embedded messaging feature in Liberty. It is a composable, flexible, and dynamic JMS messaging engine that runs within Liberty. Liberty messaging is both JMS 1.1 and JMS 2.0 specifications compliant and supports both the point-to-point and publish/subscribe messaging models.

Liberty messaging runs only in the Liberty run time, and you can use the Liberty feature manager to enable or disable the messaging features as required. Because the messaging run time is highly composable, you can enable the basic messaging features for the run time, and dynamically enable more messaging features, such as security, transactions, and remote communication, based on your requirement.

Liberty messaging can be classified into two parts:

- JMS Server run time: Provides all the runtime capabilities for connections, transactions, persistence, security, and so on.
- JMS Client connectivity: Provides the resource adapter support to allow JMS clients to perform synchronous and asynchronous messaging activities.

The messaging engine runs as a singleton instance in a Liberty, which means that at any specific time, there can be only one messaging engine that is running in a Liberty kernel.

## Liberty messaging architecture

Liberty messaging is highly composable and dynamic in nature. Liberty messaging consists of several other internal messaging subcomponents, which are implemented as OSGi bundles, that can be enabled or disabled based on the user requirements. OSGi services are used to manage component lifecycles and the injection of dependencies and configurations.

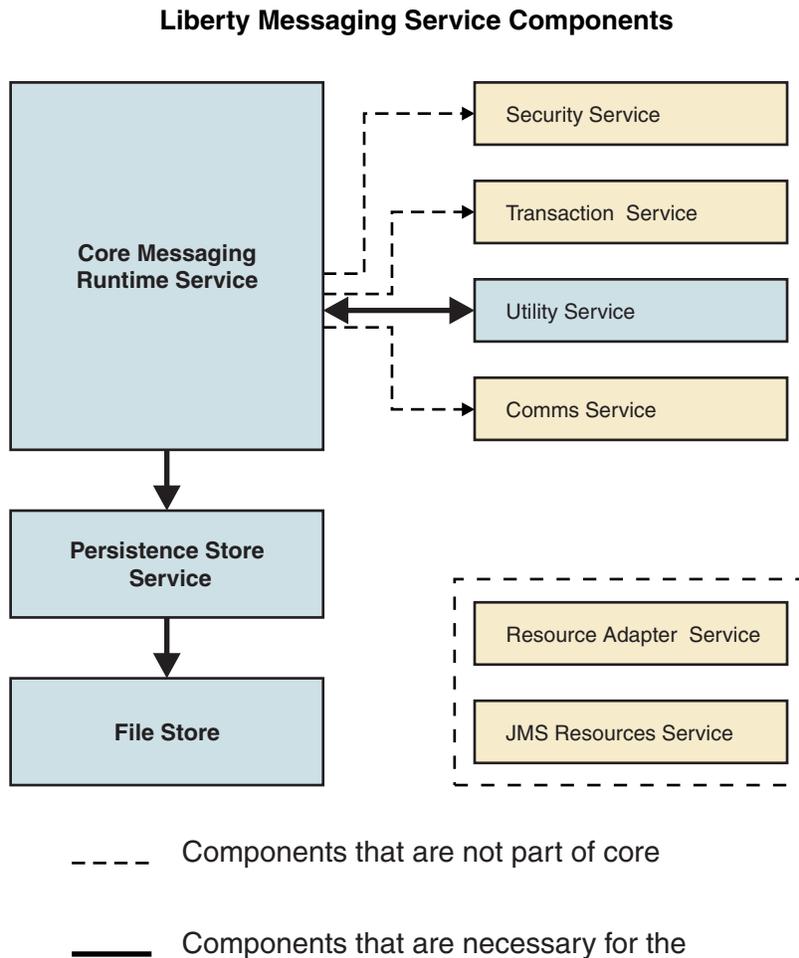


Figure 15. Liberty messaging architecture

The messaging run time and the other messaging subcomponents are run as OSGi bundles in an OSGi framework. This enables the Liberty kernel to load or unload the messaging bundles based on the usage. For example, if the user does not use the messaging security, then the bundles that are related to the messaging security are not initialized.

## Application deployment

Liberty messaging supports three types of JMS application connectivity. The application can run in any of the following ways:

- In a Liberty that is hosting the messaging engine.
- In a different Liberty that is not hosting any messaging engine.
- In WebSphere Application Server traditional.

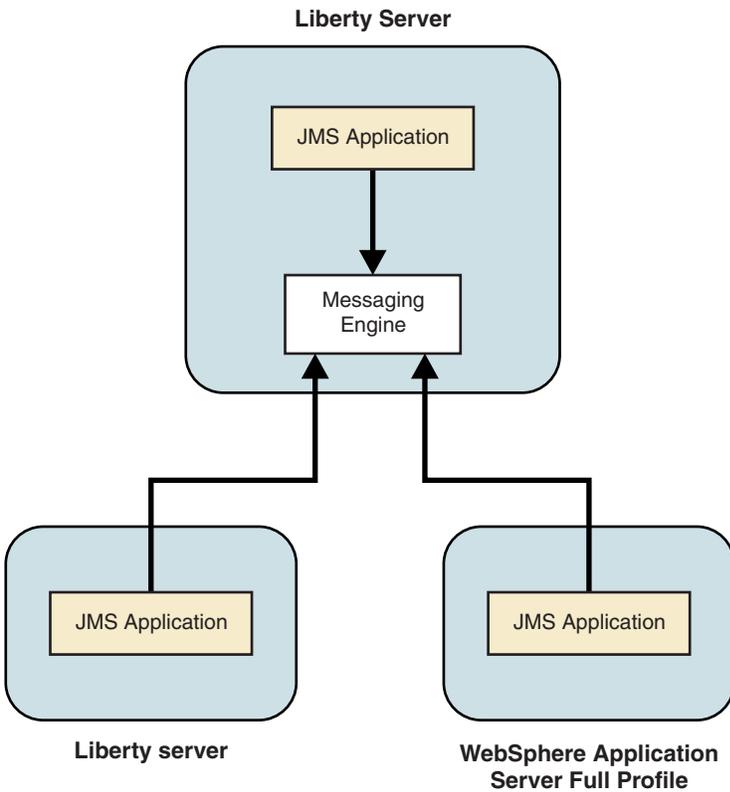


Figure 16. Application deployment model

Liberty messaging supports both *in-process* and *network TCP/IP* connectivity for applications. When the JMS application is deployed in the same JVM where the messaging engine is running, the application can communicate with the *in-process* messaging engine, without going over the TCP/IP layer. This provides significant performance benefits for the applications to send and receive messages.

JMS applications that are running on Liberty that is not hosting the messaging engine must connect over TCP/IP in order to communicate with the messaging engine.

## Message handling

Destinations (queues or topics) are always localized to the messaging engine where the destinations are defined. If the application needs to send or receive a message from a destination, it must always connect to the messaging engine that localizes the destination.

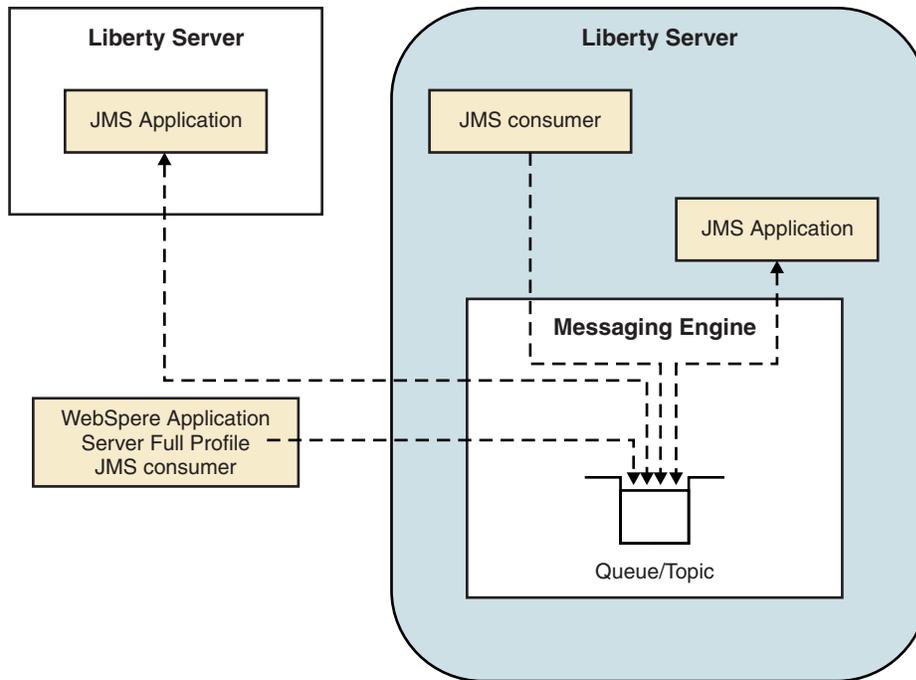


Figure 17. Message handling in Liberty messaging

## Service integration bus messaging provider



8.5.5.6

A service integration bus is a group of one or more application servers or server clusters in a WebSphere Application Server cell that cooperate to provide asynchronous messaging services. The application servers or server clusters on a bus are known as bus members. In the simplest case, a service integration bus consists of a single bus member, which is one application server.

The service integration bus messaging provider uses service integration functions and is part of the WebSphere Application Server runtime environment. To use the default messaging provider, your applications must connect to a service integration bus. You can assign JMS queues (for point-to-point messaging) or JMS topics (for publish/subscribe messaging) as destinations on the service integration bus.

The default messaging provider is characterized as follows:

- A service integration bus consists of messaging engines that run in WebSphere Application Server processes and dynamically connect to one another by using dynamic discovery. A messaging application connects to the bus through a messaging engine.
- Messaging engines use WebSphere Application Server clustering to provide high availability and scalability, and they use the same management framework as the rest of WebSphere Application Server.
- Bus client applications can run from within WebSphere Application Server (JMS), or run as stand-alone Java clients (using the J2SE Client for JMS) or run as clients that are not Java based (XMS).

## IBM MQ messaging provider



8.5.5.6

Through the IBM MQ messaging provider in Liberty, Java Message Service (JMS) messaging applications can use your IBM MQ system as an external provider of the JMS messaging resources. IBM MQ is both JMS 1.1 and JMS 2.0 specifications compliant.

You can configure IBM MQ resources for applications (for example queue connection factories) and manage messages and subscriptions that are associated with JMS destinations in Liberty. You can administer security through IBM MQ. Additional configuration might be required in IBM MQ, depending on the resources that are used by your application.

IBM MQ is characterized as follows:

- Messaging is handled by a network of queue managers, each running in its own set of processes and having its own administration.
- Features such as shared queues (on IBM MQ for z/OS) and IBM MQ clustering simplify the administration and provide dynamic discovery.
- Many IBM products and IBM partner products support IBM MQ with monitoring and control, high availability, and clustering.
- IBM MQ clients can run within WebSphere Application Server (JMS), or almost any other messaging environment by using various APIs.
- IBM MQ clients can run within a wide range of environments, platforms, and operating systems that are using various APIs. Integration through the IBM MQ resource adapter provides connectivity to other Java EE systems.

**Notes:**  The IBM MQ feature that is deployed within Liberty has the following restrictions:

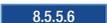
- The IBM MQ classes for Java are not supported in Liberty. They must not be used with either the IBM MQ Liberty messaging feature or with the generic JCA support. For more information, see Using WebSphere MQ Java Interfaces in J2EE/JEE Environments.
-  The IBM MQ resource adapter has a transport type of BINDINGS\_THEN\_CLIENT. This transport type is not supported within the IBM MQ Liberty messaging feature.
-  The Advanced Messaging Security (AMS) feature is not included in the IBM MQ Liberty messaging feature.

## Practical example

The “Connecting WebSphere Application Server Liberty to IBM MQ” scenario provides a worked example of using WebSphere Application Server Liberty and IBM MQ connected together. The scenario description contains the instructions to implement a solution in a business context, and to learn as you go, without needing to make use of other information resources. You can find the Connecting WebSphere Application Server Liberty to IBM MQ scenario in the product documentation.

## JMS messaging (wasJmsClient-2.0) behavior changes



 8.5.5.6

If you are using the wasJmsClient-1.1 feature in your JMS messaging applications, then you can continue to use wasJmsClient-1.1 to avoid migrating the applications. If you are creating new JMS messaging applications, then you can use the wasJmsClient-2.0 feature to take advantage of the new capabilities available. If you want to migrate your existing applications to use the wasJmsClient-2.0 feature, be aware of behavior changes that affect some of the APIs in Java Platform, Enterprise Edition 7.

The following table shows some of the differences in the behavior of the APIs between the two versions:

Table 10. Behavior differences between *wasJmsClient-1.1* and *wasJmsClient-2.0*

Interface names	Condition for exceptions	wasJmsClient-1.1	wasJmsClient-2.0
Session.createDurableSubscriber	ClientID is not set	InvalidClientIDException	IllegalStateException
TopicSession.createDurableSubscriber	ClientID is not set	InvalidClientIDException	JMSEException
Connection.setClientID	Another connection with the same ClientID is already active	IllegalStateException	InvalidClientIDException

## Java Persistence API (JPA)

8.5.5.6

Data Persistence is a means for an application to persist and retrieve information from a non-volatile storage system. Persistence is vital to enterprise applications because of the required access to relational databases. Applications that are developed for this environment must manage persistence themselves or use third-party solutions to handle database updates and retrievals with persistence. The Java Persistence API (JPA) provides a mechanism for managing persistence and object-relational mapping and functions since the EJB 3.0 specifications.

The JPA specification defines the object-relational mapping internally, rather than relying on vendor-specific mapping implementations. JPA is based on the Java programming model that applies to Java Enterprise Edition (Java EE) environments, but JPA can function within a Java SE environment for testing application functions.

JPA represents a simplification of the persistence programming model. The JPA specification explicitly defines the object-relational mapping, rather than relying on vendor-specific mapping implementations. JPA standardizes the important task of object-relational mapping by using annotations or XML to map objects into one or more tables of a database. To further simplify the persistence programming model:

- The EntityManager API can persist, update, retrieve, or remove objects from a database.
- The EntityManager API and object-relational mapping metadata handle most of the database operations without requiring you to write JDBC or SQL code to maintain persistence.
- JPA provides a query language, extending the independent EJB querying language (also known as JPQL), that you can use to retrieve objects without writing SQL queries specific to the database that you are working with.

JPA is designed to operate both inside and outside of a Java Enterprise Edition (Java EE) container. When you run JPA inside a container, the applications can use the container to manage the persistence context. If there is no container to manage JPA, the application must handle the persistence context management itself. Applications that are designed for container-managed persistence do not require as much code implementation to handle persistence, but these applications cannot be used outside of a container. Applications that manage their own persistence can function in a container environment or a Java SE environment.

Java EE containers that support the EJB 3.x programming model must support a JPA implementation, also called a persistence provider. A JPA persistence provider uses the following elements to enable easier persistence management in an EJB 3.x environment:

### Persistence unit

Defines a complete Object-Relational Model mapping Java classes (entities + supporting structures) with a relational database. The EntityManagerFactory uses this data to create a persistence context that can be accessed through the EntityManager.

### EntityManagerFactory

Used to create an EntityManager for database interactions. The application server containers

typically supply this function, but the `EntityManagerFactory` is required if you are using JPA application-managed persistence. An instance of an `EntityManagerFactory` represents a Persistence context.

### Persistence context

Defines the set of active instances that the application is manipulating currently. You can create the persistence context manually or through injection.

### EntityManager

The resource manager that maintains the active collection of entity objects that are being used by the application. The `EntityManager` handles the database interaction and metadata for object-relational mappings. An instance of an `EntityManager` represents a Persistence context. An application in a container can obtain the `EntityManager` through injection into the application or by looking it up in the Java component name-space. If the application manages its persistence, the `EntityManager` is obtained from the `EntityManagerFactory`.

### Entity objects

A simple Java class that represents a row in a database table in its simplest form. Entities objects can be concrete classes or abstract classes. They maintain states by using properties or fields.

## Java Persistence API (JPA) feature overview



8.5.5.6

There are two JPA features that you can use for your application. `jpa-2.0` is built on the Apache OpenJPA open source project. `jpa-2.1` is built on the EclipseLink open source project.

- `jpa-2.0`
- `jpa-2.1`
- JPA feature compatibility

### jpa-2.0

Java Persistence API (JPA) 2.0 for WebSphere Application Server is built on the Apache OpenJPA 2.2.x open source project.

Apache OpenJPA is a compliant implementation of the JPA 1.0 and 2.0 specifications. Using OpenJPA as a base implementation, WebSphere Application Server employs extensions to provide more features and utilities for WebSphere Application Server customers. Because JPA for WebSphere Application Server is built from OpenJPA, all OpenJPA function, extensions, and configurations are unaffected by the WebSphere Application Server extensions. You do not need to make changes to OpenJPA applications to use these applications in WebSphere Application Server.

JPA for WebSphere Application Server provides more than compatibility with OpenJPA. JPA for WebSphere Application Server contains a set of tools for application development and deployment. Other features of JPA for WebSphere Application Server include support for DB2<sup>®</sup> Optim pureQuery Runtime, DB2 optimizations, JPA Access Intent, enhanced tracing capabilities, command scripts, and translated message files. The provider of JPA for this product is `com.ibm.websphere.persistence.PersistenceProviderImpl`.

Apache OpenJPA supports the use of properties to configure the persistent environment. You can specify JPA for WebSphere Application Server properties with either the `openjpa` or `wsjpa` prefix. You can mix the `openjpa` and `wsjpa` prefixes as you want for a common set of properties. Exceptions to the rule are the `wsjpa` specific configuration properties, which use the `wsjpa` prefix. When a JPA for WebSphere Application Server-specific property is used with the `openjpa` prefix, a warning message is logged indicating that the offending property is treated as a `wsjpa` property. The reverse does not hold true for the `openjpa` prefix. In that case, the offending property is ignored.

## jpa-2.1

Java Persistence API (JPA) 2.1 for WebSphere Application Server is built on the EclipseLink open source project. EclipseLink is the reference implementation for all version of the JPA specification. The provider of JPA for this product is `org.eclipse.persistence.jpa.PersistenceProvider`.

The JPA 2.1 specification added new features that are not available in the JPA 2.0 specification. These features include:

- Schema generation
- Type conversion methods
- Entity graphs in queries and find operations
- Unsynchronized persistence contexts
- Stored procedure invocation
- Injection into Entity listener classes
- JPQL enhancements
- Criteria API enhancements
- Mapping of native queries

Refer to the JPA 2.1 specification for more details on these features. This product also provides a subset of the EclipseLink APIs. See the Liberty feature page, Java Persistence API 2.1, for details.

**Note:** JPA 2.1 is backwards compatible with JPA 2.0.

## JPA feature compatibility

### jpa-2.0

The `jpa-2.0` feature is the JPA 2.0 specification implementation and is backed by Apache OpenJPA. This feature is a part of the Java Platform, Enterprise Edition (Java EE) 6 family of technologies, but it is special as it is compatible with other Java EE 7 features. For example, the `servlet-3.1` feature, an Java EE 7 feature, is used with the `jpa-2.0` feature. This enables applications to stay with the existing JPA provider, but also use new Java EE 7 features.

### jpa-2.1

The `jpa-2.1` feature is the JPA 2.1 specification implementation and is backed by EclipseLink. This feature is only compatible with other Java EE 7 features. If the `jpa-2.1` feature is used with other Java EE 6 features, the following error is emitted into the `message.log` file.

```
CWWKF0033E: The singleton features com.ibm.websphere.appserver.javaeeCompatible-7.0 and com.ibm.websphere.appserver
```

## Java Persistence API 2.1 behavior changes

8.5.5.6

If you already use the `jpa-2.0` feature for your applications, you are encouraged to continue using the `jpa-2.0` feature for your existing applications to avoid any migration issues. For new applications, you are encouraged to use the `jpa-2.1` feature, which enables you to take advantage of the new features available in the JPA 2.1 specification. If you want to change your existing applications to use the `jpa-2.1` feature instead of the `jpa-2.0` feature, you might need to adjust your application in the migration process.

### Differences between `jpa-2.0` and `jpa-2.1`

There are a few major differences between the `jpa-2.0` and `jpa-2.1` features that you need to be aware of:

#### PersistenceProvider class name

`jpa-2.0`

- IBM provider: `com.ibm.websphere.persistence.PersistenceProviderImpl`
  - OpenJPA provider: `org.apache.openjpa.persistence.PersistenceProviderImpl`
- jpa-2.1
- `org.eclipse.persistence.jpa.PersistenceProvider`

### Caching behavior

jpa-2.0: Caching is disabled by default. If your application needs to take advantage of a L2 cache, you must explicitly enable it.

jpa-2.1: By default, the EclipseLink provider has the L2 cache and QueryCache enabled. You must ensure that this setting is the best option for your applications. If you are running in a distributed environment, like a cluster, you need to disable the cache, or understand that different nodes can have different data.

### Enhancement / weaving differences

jpa-2.0: OpenJPA requires entities to be enhanced. See the documentation on the enhancement of JPA entities for more information.

jpa-2.1: EclipseLink works with unenhanced entities. WebSphere Application Server supports static enhancement.

Some features might be unavailable, such as lazy loading and some performance gains.

- If entities classes are statically enhanced for use with the jpa-2.0 (OpenJPA) provider, the classes must be recompiled before you use the jpa-2.1 provider.

### Data source usage differences

The jpa-2.0 feature sparingly uses the non-jta-datasource, so few non-jta-datasource connections are required when you are tuning an application.

The jpa-2.1 uses a non-jta-datasource connection when reading data and a transaction is not active. This means that non-jta-datasource connection pools need to be larger when you use this feature.

See the OpenJPA -> EclipseLink migration guide page for more differences between the two JPA providers.

## JPA 2.1 features available in OpenJPA

OpenJPA, the JPA 2.0 provider, has features that function similarly to the new JPA 2.1 features. This means that if you have an existing application that uses the jpa-2.0 feature and want to use some of the JPA 2.1 new features, you do not have to switch to the jpa-2.1 feature. Instead, you can use the equivalent of the new feature that is provided by OpenJPA. Some of the key JPA 2.1 features that are available in OpenJPA are:

### Schema Generation

This feature enables you to generate DDL or interact directly with the database to define table schemas based on JPA entity definition. For more information, refer to section 9.4 of the JPA 2.1 Specification.

OpenJPA equivalent feature: Schema Mapper

### Entity Graphs

This feature enables you to specify fetching or processing of a graph of entity objects. For more information, refer to section 3.7 of the JPA 2.1 Specification.

OpenJPA equivalent feature: FetchPlan and FetchGroup

### Stored Procedure Queries

This feature enables you to invoke procedures stored in databases. For more information, refer to section 3.10.17 of the JPA 2.1 Specification.

OpenJPA equivalent feature: Query invocation

### Basic Attribute Type Conversion

This feature enables you to convert between an attribute entity representation and database representation for basic type attributes. For more information, refer to section 3.8 of the JPA 2.1 Specification.

OpenJPA equivalent feature: Externalizer feature

### @Index and @ForeignKey annotations

Refer to sections 11.1.19 and 11.1.23 of the JPA 2.1 Specification.

OpenJPA equivalent feature: OpenJPA's @Index and @ForeignKey

### Unwrap utility methods for EntityManager, Cache

Refer to sections 3.1.1 and 7.10 of the JPA 2.1 Specification.

OpenJPA equivalent features: EntityManagerImpl.unwrap() and OpenJPAPersistence.cast()

### Object construction when mapping results from native SQL

Refer to Section 3.10.16.2.2 of the JPA 2.1 Specification.

OpenJPA equivalent feature: ResultShape object

---

## Liberty profile: Process types on z/OS

z/OS

For the Liberty runtime environment on the z/OS platform, there are two types of process: the server process and the angel process.

### Server process (bbgzsrv)

The server process is a Java virtual machine (JVM) running the Liberty code in much the same way as it does on any other operating system. You can start the server process either from the MVS operator console by using the angel process or from the shell. How a user identity is associated and validated depends on how you start the server:

- If you start the server from an operator console, the identity that is associated with the STARTED profile created by using a z/OS security product such as RACF<sup>®</sup> is used to control server access: `start bbgzsrv,parms='defaultServer'`
- If you start the server from the shell, you must also stop the server from the shell. The identity of the shell is used for the server:

```
server start
server stop
```

The JVM start options for the server process can come from three sources:

- If you define a file name in the JAVA\_OPTS DD in the proc for the server process, Java command-line arguments are read from this file.
- If you do not define a file name in the JAVA\_OPTS DD, Java command-line arguments are read from the `jvm.options` file in the server configuration directory.
- If the `jvm.options` file does not exist, the JVM uses the value of the `IBM_JAVA_OPTIONS` environment variable.

### Angel process (bbgzangl)

The angel process runs in an authorized key and provides facilities to server process to load and

access system services in a way that protects the integrity of the operating system. You start the angel process from the MVS console by using a proc.

The angel does not need any configuration and exists independently of the server. All Liberty servers that are running on a z/OS image can share a single angel, regardless of the level of code that the servers are running.

Use the MODIFY command to give a list of all the servers that are using the angel process.

```
MODIFY [jobname.]identifier,display,servers
```

If no z/OS system authorized services are enabled for any server on a system, the angel does not need to be active. The angel process is not required for the command processing services (the command processing services uses unauthorized z/OS services for command support).

If the server is configured to attempt to use authorized services but either the angel is not available, or if the effective owner of the process is not authorized to use the angel, the authorized service is not available to be used on that server. In some cases, an unauthorized service might be used instead. See “Liberty: Unauthorized services used by the SAF registry” on page 1946.

For more information, see “Administering Liberty on z/OS” on page 1731

## IBM z/OS Connect overview



8.5.5.2

The IBM z/OS Connect offering is a Liberty feature that encapsulates calling z/OS target applications using REST (Representation State Transfer) calls.

z/OS Connect is designed to provide a fast, secure, reliable connector to reach any z/OS asset. z/OS Connect provides a standard way to identify these assets and reach the assets using REST technology. Where these assets run is specified in the z/OS Connect configuration, relieving clients applications in the cloud, mobile, and web worlds of the need to understand the details about how to reach them and how to convert payloads to and from the formats that the applications require.

### Benefits of using z/OS Connect

z/OS Connect adds value for z/OS customers by enabling users to consolidate multiple client connect pathways into a single common gateway or concentrator for synchronous calls to reach business assets and data on z/OS operating systems. Virtually any z/OS asset, applications and data, can be reached by using standard REST HTTP calls. This feature also provides the ability to inquire about, or discover, all assets that are defined in the z/OS Connect configuration repository. The following is a summary of the benefits of z/OS Connect:

- Provides RESTful access to identify and invoke z/OS-based business assets in CICS®, IMS™, UNIX System Services, and traditional batch environments, opening up these assets to cloud and mobile-based system of engagement environments.
- Functionality that is based on Liberty server technology, is lightweight and easily configurable, and provides z/OS differentiation with System Authorization Facility (SAF) security integration, z/OS Workload Manager (WLM), and Resource Recovery Services (RRS) integration. WLM integration means different URIs can have varying levels of priority and performance criteria.
- As a feature in the Liberty server on z/OS, you can integrate z/OS Connect with z/OS standard system management, which can run as a started task and integrate with z/OS automated operations.
- Provides the ability to secure individual or groups of z/OS Connect services with SAF security in which only specific users or groups can have access to specific services.
- Provides the ability to uniformly track requests from cloud, mobile, and web environments by using z/OS System Management Facility (SMF) services. This tracking means that z/OS customers can use their existing processes for auditing and chargeback for requests from these environments.

- Enables the ability to do an automatic conversion of the request payload from JavaScript Object Notation (JSON) form on input to binary form consumable by z/OS applications such as Cobol, PL/I, and C. The reverse for the response from the z/OS application, converting the output from binary to JSON form is also true.

## **z/OS Connect terminology**



8.5.5.2

Become familiar with terms used with z/OS Connect that include Systems of Engagement (SoE), Systems of Record (SoR), and REST concepts.

### **Systems of Engagement and Systems of Record**

The terms Systems of Engagement (SoE) and Systems of Record (SoR) have replaced the older client and server terminology when describing how different systems are classified in the cloud environment. IBM® z/OS® Connect provides the tools that are needed to transform requests from SoE environments to applications that are running on SoR servers on the z/OS operating system.

### **RESTful services**

REST is an acronym for Representational State Transfer, or the pattern that is most commonly used for web requests today that run over the HTTP protocol. The REST protocol relies solely on the HTTP GET/PUT/POST/DELETE methods. A concrete implementation of a RESTful service must provide the following:

- Explicit use of HTTP
- Stateless functionality
- Displays directory structure-like URIs
- Support Transfer XML, JavaScript Object Notation (JSON), or both

IBM z/OS Connect provides a set of RESTful services that offer discovery and linkage from external cloud, mobile, and web environments to business assets on z/OS systems. Use a RESTful HTTP GET request to return a list of services that the target z/OS Connect server has under its management and another GET request to return the information about a single service, such as the service provider that it uses, like WOLA, and the other artifacts that are needed to invoke, or call, the asset. An HTTP POST or PUT request is used to invoke the asset, by passing a request payload to the asset and returning a response.

## **z/OS Connect scenarios**



8.5.5.2

IBM® z/OS Connect offers REST-based access to applications and data with JSON-based payloads. This access pattern has gained great favor in the industry.

The following business scenarios describe various benefits of using z/OS Connect:

### **Consolidating or grouping separate requests (Financial services company scenario)**

A financial services firm that recently completed a merger with another firm is looking for a way to provide a secure and fast way to open up several critical business applications and tie them together to form a single result and make the result available from inside a web application. One z/OS application, called ACCTINFO runs in the CICS® environment and provides access to internal account data for customers. A second application, ACCTHSTY, runs in the IMS™ environment. The data managed by the CICS application is stored in Virtual Storage Access Method (VSAM) files. The IMS data is in DL/I tables.

The company has a requirement to unify the security for accessing these applications and be able to identify when and how many calls to these two applications occur, the number of bytes received and returned, as well as the response time.

z/OS Connect offers a simple solution that hides the complexity of these environments behind its configuration. The solution provides the ability to contact a single server running on a z/OS operating system to call in to both applications using REST-based calls and JSON for the message payloads. The data transformation support that is provided in z/OS Connect handles the mapping both to and from JSON and byte arrays for each request. In addition, z/OS Connect provides the single point for security checking to ensure any ID systems requesting access are authorized to reach these applications and it records each REST call in the z/OS system management facility (SMF). For unifying these requests, z/OS Connect service definitions use the `serviceGroupName` string when each of these services are defined in the z/OS Connect configuration. You can set up the `serviceGroupName` data to be common for each service, such as 'ACCOUNT\_INFO\_HISTORY' and the result appears in the z/OS SMF records for each request enabling them to be correlated together for analysis or chargeback purposes.

### **Separating mobile or web requests scenario (Retail scenario)**

A retailer wants to separate web requests to applications on z/OS systems out from requests that are coming from their new mobile platforms. You can easily accomplish this task by defining and configuring distinct z/OS Connect service definitions to use the same service provider configuration which enables multiple REST services to call the same assets, but the calls are recorded and secured with different criteria. Requesters from mobile platforms are authorized to use one set of services using REST, while calls from non-mobile, web-based requesters are authorized to use a separate set, both accessing the same assets but tracked separately. All the data is recorded in the z/OS Connect SMF 120 subtype 11 records and are accessible by using standard z/OS auditing and tracking mechanisms.

### **Reaching traditional z/OS batch assets by using REST and JSON (Insurance company scenario)**

A large insurance firm wants to reach a set of Cobol batch applications that contains some sophisticated business logic that was developed over many years. Conversion of this application to a newer language and runtime environment would be costly and high risk. A solution to access the business logic in this application from mobile and web-based requesters is much less risk and enables other business systems to take advantage of the established applications.

With the WebSphere® Optimized Local Adapters support in Liberty and the z/OS Connect WOLA feature activated, this application can be reached using REST calls and JSON content with little effort. The target Cobol application program requires updates to use the WOLA APIs to register with the Liberty server and start accepting requests. A z/OS Connect service definition is required, as well as the binding file that contains the information about the data it expects to receive. You must copy the return data to the path of the binding file of the z/OS Connect server. After enabling the use of the z/OS Connect and the WOLA APIs, this batch asset is effectively online and available for authorized z/OS Connect REST clients.

### **Discovery of z/OS assets and information about request and response payloads**

You want your cloud provisioning or API management tool needs to generate a catalog of assets that are published on a specific z/OS system. This tool needs to inquire about these assets and store them, along with some context associated with each asset. The tool also must include information about what is required to create request data that is passed to the service and information about what the service returns as the response.

z/OS Connect offers a way to discover all the services in its configuration with a simple REST call. When an HTTP GET request arrives for `https://host:port/zosConnect/services`, a list in JSON form is returned and contains all the services that the current authenticated user is permitted to see. From this

list, you can retrieve the URLs for each service and query each service by using an HTTP GET to return the request and response JSON schema information. You can save the service reference (URL for the service), service textual description, and the JSON request and response schemas in the tool's catalog for retrieval at a later time. Enabling access to the JSON schema means that the tool might easily be configured to generate a REST call to pass to z/OS Connect, with an appropriate JSON-based parameter list, for use by the target z/OS Connect service.

---

## Liberty:Binary logging

8.5.5.0

Binary logging is a high performance log and trace facility based on the High Performance Extensible Logging (HPEL) technology in WebSphere Application Server traditional.

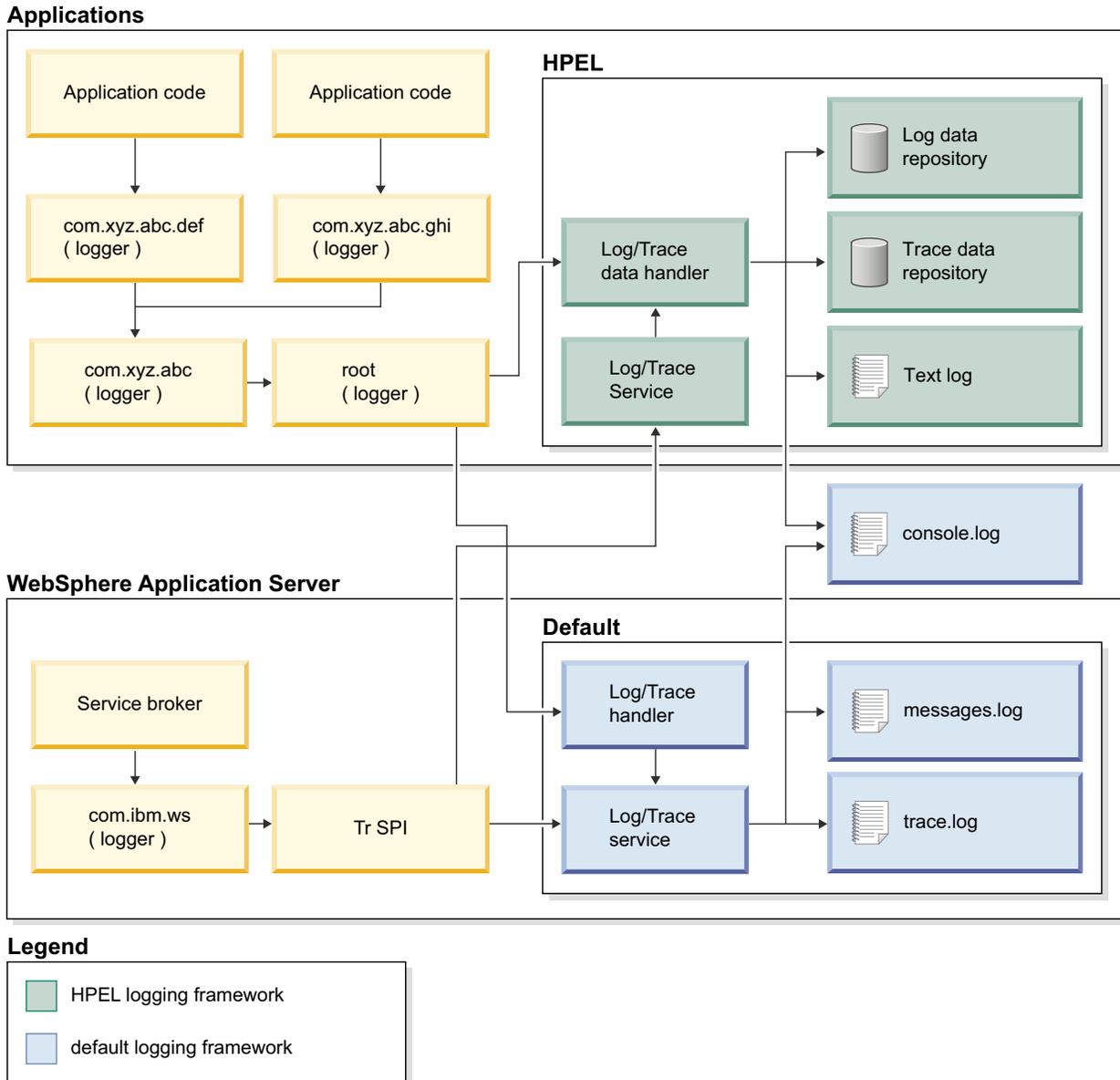
### Overview

**Note:** You must enable the binary logging facility to use it.

Binary logging provides a convenient mechanism for storing and accessing log, trace, System.err, and System.out information produced by the application server or your applications. It is an alternative to the default log and trace facility, which provides the JVM logs and diagnostic trace files commonly named messages.log and trace.log.

### Log and trace storage

Binary logging provides a log data repository and a trace data repository. See the following figure to understand how applications and the application server store log and trace information.



### Log data repository

The log data repository is a storage facility for log records. Log data is typically intended to be reviewed by administrators. This includes any information applications or the server write to System.out, System.err, OSGi logging service at level LOG\_INFO or higher (including LOG\_INFO, LOG\_WARNING, and LOG\_ERROR), or java.util.logging at level Detail or higher (including Detail, Config, Info, Audit, Warning, Severe, Fatal, and any custom levels at level Detail or higher).

### Trace data repository

The trace data repository is a storage facility for trace records. Trace data is typically intended for use by application programmers or by the WebSphere Application Server support team. This includes any information applications or the server write to the OSGi logging service at level LOG\_DEBUG or java.util.logging at levels below level Detail (including Fine, Finer, Finest, and any custom levels below level Detail).

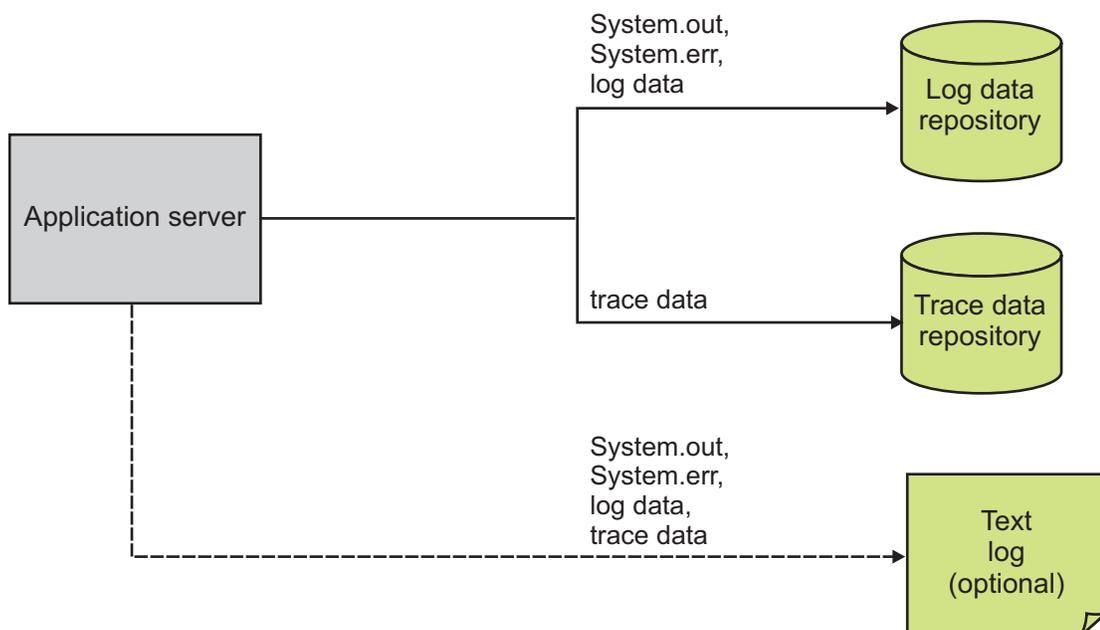
## Log and trace performance

Binary logging has been designed and tested to significantly outperform the default log and trace facility. One result is that the application server can run with trace enabled while causing less impact to performance than tracing the same components using the default log and trace framework. Another result is that applications that frequently write to the logs can run faster when using binary logging.

### Log and trace events are each stored in only one place

Log events, System.out, and System.err are stored in the log data repository. Trace events are stored in the trace data repository. Storing each type of event in only one place ensures that performance is not wasted on redundant data storage.

**Note:** The console log should be disabled in cases where logging performance is important. Any content written to the console log will already be stored in the log data repository.



### Data is not formatted unless it is needed

Formatting data for a user to read uses processor time. Rather than format log event and trace event data at run time, log and trace data are stored more rapidly in a proprietary binary representation. This improves the performance of the log and trace facility. By deferring log and trace formatting until the `binaryLog` command is run, sections of the log or trace that are never viewed are never formatted.

### Log and trace data are buffered before being written to disk

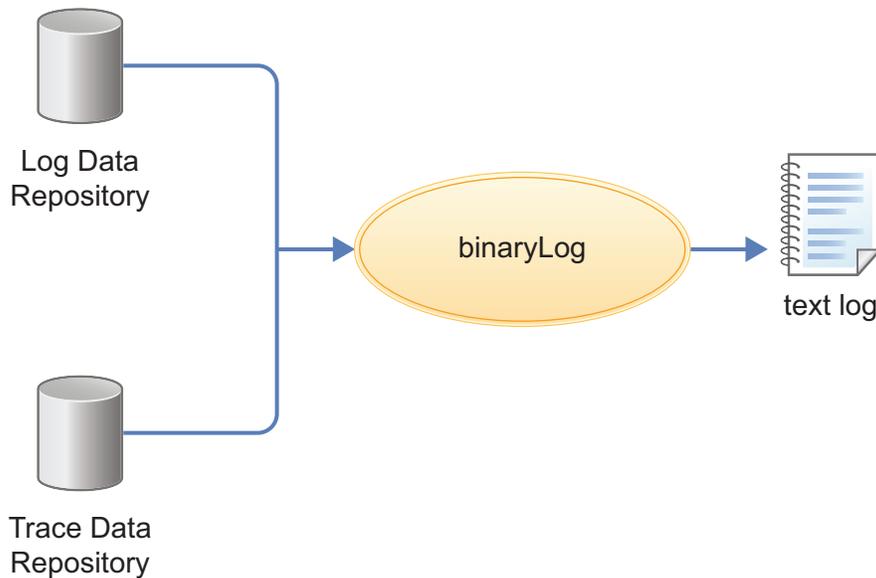
Writing large blocks of data to a disk is more efficient than writing the same amount of data in small blocks. The binary logging facility provides the capability to buffer log and trace data before writing it to disk. By default, log and trace data are stored in an 8 KB buffer before being written to disk. If the buffer is filled within 10 seconds, the buffer is written to disk. If the buffer is not filled within that time it is automatically written to disk to ensure that the logs have the most current information.

## Administration of log and trace

Binary logging has been designed to be easy to configure and understand. For example, administrators can easily configure how much disk space to dedicate to logs or trace, or how long to retain log and trace records, and leave the management of log and trace content up to the server. As another example all log, trace, System.out, and System.err content can be accessed using one easy-to-use command (`binaryLog`), avoiding any possible confusion over which file to access for certain content.

### Reading from the log data and trace data repositories

The log data and trace data repositories are stored in a WebSphere Application Server proprietary format and cannot be read using text file editors such as Notepad or VI. You can copy the log data and trace data repositories in to a plain text format using the `binaryLog` command.



### `binaryLog` command

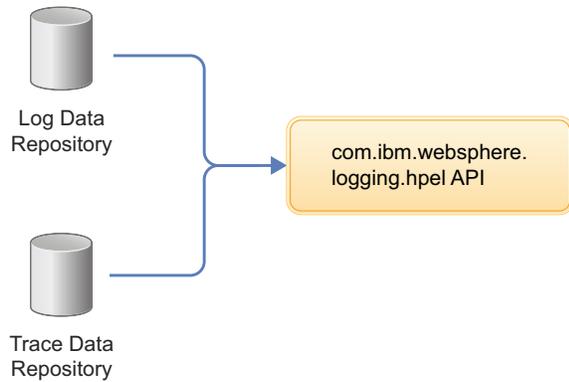
`binaryLog` is an easy-to-use command-line tool provided for users to work with the log data and trace data repositories. `binaryLog` provides filtering and formatting options that make finding important content in the log data and trace data repositories easy. For example, a user might filter any errors or warnings, then filter all log and trace entries that occurred within 10 seconds of a key error message on the same thread.

### Filtering using log and trace record extension content

The binary logging facility provides the capability for developers to add custom extensions to log and trace records using a log record context API (`com.ibm.websphere.logging.hpel.LogRecordContext`). You can use the `binaryLog` command-line tool to filter records based on the content of log and trace record extensions.

## Development resources

Binary logging has been designed to make working with log and trace content more flexible and effective than the default logging facility. Log and trace content can be easily filtered to show only the records that are of interest. You can use the command line (see the description of the `binaryLog` command), or developers can create powerful log handling programs using the HPEL API.



### Reading the log data and trace data

An API has been provided to make it easy for developers to develop tools to consume content from the binary log and trace repositories. For example, a developer might write a Java program to search the log and trace content to find any messages with message IDs that match a known list of important message IDs. This API is in the `com.ibm.websphere.logging.hpel` package. Refer to the API documentation for details on the HPEL log reading API.

### Log and trace record extensibility

Developers can add custom extensions to log and trace records through a log record context API (`com.ibm.websphere.logging.hpel.LogRecordContext`). When binary logging stores log and trace records, it includes any extensions present in the log record context on the same thread. For example, a developer might write a servlet filter to add important HTTP request parameters to the log record context. While that servlet runs, HPEL API adds those extensions to any log and trace records created on the same thread.

As with other log and trace record fields, developers can access the record extensions using the HPEL API. This is useful when writing tools to read from log and trace repositories. Developers can also make use of the log record context API to access extensions in custom log handlers, filters, and formatters at run time.

## BinaryLog command options

**8.5.5.0**

Use the **binaryLog** command to view or copy the contents of a binary logging repository, or list the available server process instances in the repository. The **binaryLog** command is equivalent to the **logViewer** command in the profile bin directory of the traditional application server.

The binary log and trace facility writes to a repository in a binary format. You can view, query and filter the repository using the **binaryLog** command. The **binaryLog** command provides options for quickly converting repository contents into a text file in various formats, such as basic and advanced formats. The command also provides options to make getting the data you need from the logs easier; for example, allowing you to filter what log records you want by level, logger name, or date and time.

### Syntax

The command syntax is as follows:

```
binaryLog action {serverName | repositoryPath} [options]
```

The value of **options** is different based on the value of **action**.

## Parameters

The following actions are available for the binaryLog command:

### view

Read a repository, optionally filter it, and create a version that users can read.

The command syntax is as follows:

```
binaryLog view {serverName | repositoryPath} [options]
```

*serverName*

Specify the name of a Liberty server with a repository to read from.

*repositoryPath*

Specify the path to a repository to read from. This is typically the directory that contains both the logdata and tracedata directories.

**Note:** If neither a *serverName* nor a *repositoryPath* is specified on the command line, the task is performed against the default server instance, `defaultServer`, if it exists.

Filter options:

All filters are optional. When multiple filters are used, they are logically ANDed together.

- `--minDate=value`  
Filter based on minimum record creation date. Value must be specified as either a date (for example `--minDate="2/20/13"`) or a date and time (for example `--minDate="2/20/13 16:47:21:445 EST"`).
- `--maxDate=value`  
Filter based on maximum record creation date. Value must be specified as either a date (for example `--maxDate="2/20/13"`) or a date and time (for example `--maxDate="2/20/13 16:47:21:445 EST"`).
- `--minLevel=value`  
Filter based on minimum level. Value must be one of FINEST | FINER | FINE | DETAIL | CONFIG | INFO | AUDIT | WARNING | SEVERE | FATAL.
- `--maxLevel=value`  
Filter based on maximum level. Value must be one of the following: FINEST | FINER | FINE | DETAIL | CONFIG | INFO | AUDIT | WARNING | SEVERE | FATAL.
- `--includeLogger=value[,value]*`  
Include records with specified logger name. Value may include \* or ? as a wildcard.
- `--includeMessage=value`  
Filter based on message name. Value may include \* or ? as a wildcard.
- `--includeThread=value`  
Include records with specified thread id. Values must be in hexadecimal (for example, `--includeThread=2a`).
- `--includeExtension=name=value[,name=value]*`  
Include records with specified extension name and value. Value may include \* or ? as a wildcard. To include a comma in the value, you must use "\",
- `--includeInstance=value`  
Include records from the specified server instance. Value must either be "latest" or be a valid instance ID. Run this command using the `listInstances` action to see a list of valid instance IDs.

Monitor option:

--monitor

Continuously monitor the repository and output new content as it is generated.

Output options:

- --format={basic | advanced | CBE-1.0.1}  
Specify the output format to use. "basic" is the default format.
- --encoding=*value*  
Specify the character encoding to use for output.

## copy

Read a repository, optionally filter it, and write the contents to a new repository.

The command syntax is as follows:

```
binaryLog copy {serverName | repositoryPath} targetPath [options]
```

*serverName*

Specify the name of a Liberty server with a repository to read from.

*repositoryPath*

Specify the path to a repository to read from. This is typically the directory that contains the logdata and tracedata directories.

*targetPath*

Specify the path at which to create a new repository. The *targetPath* must be specified.

**Note:** Either *serverName* or *repositoryPath* must be specified, as well as the *targetPath*.

Filter options:

All filters are optional. When multiple filters are used, they are logically ANDed together.

- --minDate=*value*  
Filter based on minimum record creation date. Value must be specified as either a date (for example --minDate="2/20/13") or a date and time (for example --minDate="2/20/13 16:52:32:808 EST").
- --maxDate=*value*  
Filter based on maximum record creation date. Value must be specified as either a date (for example --maxDate="2/20/13") or a date and time (for example --maxDate="2/20/13 16:52:32:808 EST").
- --minLevel=*value*  
Filter based on minimum level. Value must be one of the following: FINEST | FINER | FINE | DETAIL | CONFIG | INFO | AUDIT | WARNING | SEVERE | FATAL.
- --maxLevel=*value*  
Filter based on maximum level. Value must be one of the following: FINEST | FINER | FINE | DETAIL | CONFIG | INFO | AUDIT | WARNING | SEVERE | FATAL.
- --includeLogger=*value*[,*value*]\*  
Include records with specified logger name. Value may include \* or ? as a wildcard.
- --excludeLogger=*value*[,*value*]\*  
Exclude records with specified logger name. Value may include \* or ? as a wildcard.
- --includeMessage=*value*  
Filter based on message name. Value may include \* or ? as a wildcard.
- --includeThread=*value*  
Include records with specified thread id. Values must be in hexadecimal (for example, --includeThread=2a).
- --includeExtension=*name=value*[,*name=value*]\*

Include records with specified extension name and value. Value may include \* or ? as a wildcard. To include a comma in the value, you must use "\",

- `--includeInstance=value`

Include records from the specified server instance. Value must either be "latest" or be a valid instance ID. Run this command using the listInstances action to see a list of valid instance IDs.

## listInstances

List the IDs of server instances in the repository. A server instance is the collection of all log/trace records written from the time a server is started until it is stopped. Server instance IDs can be used with the `--includeInstance` option of the binaryLog view action.

The command syntax is as follows:

```
binaryLog listInstances {serverName | repositoryPath}
```

*serverName*

Specify the name of a Liberty server with a repository to read from.

*repositoryPath*

Specify the path to a repository to read from. This is typically the directory that contains the logdata and tracedata directories.

**Note:** If *serverName* or *repositoryPath* are not specified on the command line, the task is performed against the default server instance, `defaultServer`, if it exists.

Be aware of binaryLog filtering optimizations. The binaryLog tool is able to filter log and trace data most efficiently when used with the following filter options:

- `--minDate`
- `--maxDate`
- `--includeThread`
- `--minLevel`
- `--maxLevel`

## Example usage

See the following examples of binaryLog commands.

- Display all events in the `defaultServer` repository between July 19th, 2013 and August 2nd, 2013.  

```
binaryLog view --minDate=07/19/13 --maxDate=08/02/13
```
- Display new events from server `myServer`, whose specified level is `WARNING` or higher, using the advanced format as the server writes them to the log repository.  

```
binaryLog view myServer --monitor --minLevel=WARNING --format=advanced
```
- Write log messages from a repository at `/apps/server1/logs`; include only those that were written to the error stream of a specific repository.  

```
binaryLog view /apps/server1/logs --includeLogger=SystemErr
```
- View events from the `defaultServer` repository that occurred before September 14th, 2012 4:28 PM eastern daylight time.  

```
binaryLog view --maxDate="09/14/12 16:28:00:000 EDT"
```
- Write events from the `defaultServer` repository that contain a 'thread' extension with value 'Default Executor-thread-4'  

```
binaryLog view --includeExtension=thread="Default Executor-thread-4" --format=advanced
```
- View the list of server instances in the `defaultServer` repository:  

```
binaryLog listInstances
```

Using `D:\wlp\usr\servers\defaultServer\logs` as repository directory.

Instance ID	Start Date
1358809441761	1/21/13 18:04:01:761 EST
1358864476191	1/22/13 9:21:16:191 EST

1358869523192	1/22/13 10:45:23:192 EST
1358871281166	1/22/13 11:14:41:166 EST
1358879829000	1/22/13 13:37:09:000 EST
1358892222067	1/22/13 17:03:42:067 EST

- View events from the defaultServer using one of the instance IDs from the previous example:

```
binaryLog view --includeInstance=1358871281166
```

- Copy events from the defaultServer, whose specified level is WARNING or higher, from the latest server instance to a new repository at d:\toSupport directory.

```
binaryLog copy defaultServer d:\toSupport --minLevel=warning --includeInstance=latest
```

## Configuring binary logging in Liberty

8.5.5.0

Use this information as a guide for configuring binary logging in your Liberty.

### About this task

Binary logging provides faster log and trace handling capabilities and more flexible ways to use log and trace content than the default Liberty log and trace framework.

A server configuration consists of a `bootstrap.properties` file, a `server.xml` file, and any (optional) files that are included with those files. The `bootstrap.properties` file specifies properties that need to be available before the main configuration is processed, and are kept to a minimum. The `server.xml` file is the primary configuration file for the server.

The `server.xml` file and its associated files use a simple xml format that is suitable for most text editors.

**Distributed operating systems** A richer editing experience is provided by the eclipse server adapter for Liberty (WAS4D+ adapter), which uses a generated schema to provide drop-down lists of available choices, auto-completion, and other editing tools. For a description of the eclipse server adapter for Liberty, see “Editing the Liberty configuration by using developer tools” on page 1556.

The `bootstrap.properties` file specifies whether the server uses binary logging as the log and trace framework, or the default log and trace framework. A server restart is required to switch between binary logging and the default log and trace framework.

You can modify the configuration of binary logging through the server configuration or the `bootstrap.properties` file.

- **Server configuration:** To get logging from your own code, which is loaded after server configuration processing, use the server configuration to configure binary logging.
- **bootstrap.properties file:** You might need to set logging properties to take effect before the server configuration files are processed. For example, if you need to analyze problems that occur early in server start or configuration processing. In this case, you can configure binary logging in the `bootstrap.properties` file.

You can set Logging properties in either the `bootstrap.properties` or the `server.xml` file. Use attributes in the `server.xml` file, or use equivalent properties in the `bootstrap.properties` file. Any settings in the `bootstrap.properties` file are used from the time the server reads the `bootstrap.properties` file until the time the `server.xml` file is processed. If the logging properties in the `bootstrap.properties` file are not replaced or reset in the `server.xml` file, the property values in the `bootstrap.properties` file continue to be used.

When binary logging is enabled, the `maxFileSize`, `maxFiles`, `messageFileName`, `traceFileName`, and `traceFormat` logging element attributes are ignored (since binary logging runs without `trace.log` and

messages.log files). The **traceSpecification**, **consoleLogLevel**, and **logDirectory** attributes continue to be used to set the trace specification, the level for the console log, and the placement of the log and trace files.

If you set logging or binary logging attributes in the server.xml file, you can avoid changes in configuration between startup time and runtime by setting the corresponding properties in the bootstrap.properties file to the same value. If no logging or binary logging properties are set in the bootstrap.properties file, the server uses the default logging settings.

## Procedure

- Enable binary logging for the server by updating the bootstrap.properties file. In the bootstrap.properties file, add the following text on a line by itself:  
websphere.log.provider=binaryLogging-1.0
- Use the following parameters to configure binary logging. All subelements that are listed are subelements of the logging element in the server.xml file. The following table lists the attributes that are configurable in the server.xml file and the equivalent properties that can be set in the bootstrap.properties file:

*Table 11. Binary logging attributes that are configurable in server.xml and the equivalent properties that can be set in bootstrap.properties*

Logging subelement	Attribute	Equivalent bootstrap.properties property
binaryLog	purgeMaxSize	com.ibm.hpel.log.purgeMaxSize
	purgeMinTime	com.ibm.hpel.log.purgeMinTime
	fileSwitchTime	com.ibm.hpel.log.fileSwitchTime
	bufferingEnabled	com.ibm.hpel.log.bufferingEnabled
	outOfSpaceAction	com.ibm.hpel.log.outOfSpaceAction
binaryTrace	purgeMaxSize	com.ibm.hpel.trace.purgeMaxSize
	purgeMinTime	com.ibm.hpel.trace.purgeMinTime
	fileSwitchTime	com.ibm.hpel.trace.fileSwitchTime
	bufferingEnabled	com.ibm.hpel.trace.bufferingEnabled
	outOfSpaceAction	com.ibm.hpel.trace.outOfSpaceAction

The following example shows a bootstrap.properties file that is configured to enable binary logging:  
websphere.log.provider=binaryLogging-1.0

The following example shows a server.xml file with the binary logging subelements. The log content is set to expire after 96 hours and the trace content is set to retain a maximum of 1024MB:

```
<server description="new server">
  <logging>
    <binaryLog purgeMinTime="96"/>
    <binaryTrace purgeMaxSize="1024"/>
  </logging>
</server>
```

For the full logging configuration reference, see the logging, binaryLog, and binaryTrace elements in the .

## Results

After you restart the server, binary logging is enabled and configured.

---

## Liberty: Session Initiation Protocol (SIP)

8.5.5.7

Session Initiation Protocol (SIP) is a control protocol for many interactive services, including audio, video, and peer-to-peer communication. SIP, and the standards for SIP, provide the mechanisms to look up, negotiate, and manage connections to peers on any network over any other protocol.

With the sipServlet-1.1 feature, Liberty includes support for SIP Servlet Specification 1.1, also referred to as Java Specification Request (JSR) 289. The SIP Servlet Specification provides the Java API standards for Session Initiation Protocol (SIP). JSR 289 is an update to the existing SIP Servlet specification that addresses new requirements that were determined by industry users. This product continues to support the SIP Servlet 1.0 specification.

This product complies with the following SIP standards:

- IETF
- JCP

For a complete list of the supported Internet Engineering Task Force (IETF) and Java Community Process (JCP) industry standards, see the “SIP industry standards compliance on Liberty” on page 1035.

In the Liberty server, the web container and SIP container are converged and are able to share session management, security and other attributes. In this model, an application that includes SIP servlets, HTTP servlets, and portlets can seamlessly interact, regardless of the protocol. The tight integration of HTTP and SIP in the Liberty server means that these converged applications are highly available.

### Session Initiation Protocol (SIP) applications on Liberty

A *SIP application* is a Java program that uses at least one Session Initiation Protocol (SIP) servlet.

A SIP servlet is a Java application component that is managed by a SIP servlet container and that performs SIP signaling. Like other Java components, servlets are platform-independent Java classes that are compiled to platform-neutral bytecode that can be loaded dynamically into and run by a Java-enabled SIP application server such as a Liberty profile server. Containers, sometimes called servlet engines, are server extensions that handle servlet interactions. SIP servlets interact with clients by exchanging request and response messages through the servlet container.

SIP is used to establish, modify, and terminate multimedia IP sessions, including IP telephony, presence, and instant messaging. “Presence” in this context refers to user status such as “Active,” “Away,” or “Do not disturb.” The standard that defines a programming model for writing SIP-based servlet applications is JSR 289. The idea behind the specification is to provide a Java application programming interface (API) similar to HTTP servlets that provides an easy-to-use SIP programming model. Like the HTTP servlet programming model, some flexibility is limited to optimize ease-of-use and time-to-value.

However, the SIP Servlet API is different in many ways from HTTP servlets because the protocol is so different. While SIP is a request-response protocol, there is not necessarily only one response to every one request. This complexity and a need for a high-performing solution meant that it was easier to make the SIP servlets natively asynchronous. Also, unlike HTTP servlets, the programming model for SIP servlets sought to make client requests easy to create alongside the other logic because many applications act as a client or proxy to other servers or proxies.

### SipServlet requests

Like HTTP servlets, each SIP servlet extends a base `javax.servlet.sip.SipServlet` class. All messages come in through the service method, which you can extend. However, because there is not a one-to-one

mapping of requests to responses in SIP, the suggested practice is to extend the `doRequest` or `doResponse` methods instead. When you extend the `doRequest` or `doResponse` methods, it is important to call the extended method for the processing to complete.

Each request method, which the specification must support, has a `doxxx` method just like HTTP. In HTTP, methods such as `doGet` and `doPost` exist for GET and POST requests. In SIP, `doInvite`, `doAck`, `doOptions`, `doBye`, `doCancel`, `doRegister`, `doSubscribe`, `doNotify`, `doMessage`, `doInfo`, and `doPrack` methods exist for each SIP request method.

Unlike an HTTP servlet, SIP servlets have methods for each of the response types that are supported. So, SIP servlets include the `doProvisionalResponse`, `doSuccessResponse`, `doRedirectResponse`, and `doErrorResponse` responses. Specifically, the provisional responses (1xx responses) are used to indicate status, the success responses (2xx responses) are used to indicate a successful completion of the transaction, the redirect responses (3xx responses) are used to redirect the client to a moved resource or entity, and the error responses (4xx, 5xx, and 6xx responses) are used to indicate a failure or a specific error condition. These types of response messages are similar to HTTP, but because the SIP Servlet programming model includes a client programming model, responses must be handled programmatically as well.

## JSR 289 overview

8.5.5.7

With the `sipServlet-1.1` feature, Liberty includes support for SIP Servlet Specification 1.1, also referred to as Java Specification Request (JSR) 289. SIP is a signaling protocol that is used for creating, modifying, and terminating IP communication sessions, such as telephony, presence, and multimedia applications.

The SIP Servlet Specification provides the Java API standards for Session Initiation Protocol (SIP). JSR 289 is an update to the existing SIP Servlet specification that addresses new requirements that were determined by industry users.

The JSR 289 specification adds the following features:

- Application router for application selection  
Application routing enables developers to build complex services out of smaller applications. On initial requests the container calls the application router to determine which application to invoke based on the type of request. The application router is the central hub for selecting application order. For more information, see “SIP application router on Liberty” on page 1035 and “Administering Session Initiation Protocol (SIP) on Liberty” on page 1728.
- Annotation-based programming  
Annotations provide a fast way to develop applications by embedding metadata directly in applications. For example, you can use the `@SipServlet` annotation to indicate that a class is a SIP servlet. The `@SipApplication` is a package level annotation. All servlets in the package belong to the same application unless the servlet uses `@SipServlet(applicationName)`. For more information on annotations, see section 18 of the JSR 289.
- Converged applications  
JSR 289 provides a new, standardized mechanism for building converged applications. A converged application contains SIP servlet components and other Java EE components such as HTTP servlets and enterprise beans. The specification includes two new classes to support convergence.
  - `ConvergedHttpSession` is an extension to `HttpSession` for converged applications.
  - `SipSessionUtil` handles session management for converged applications.For more information on converged applications, see section 13 of the JSR 289.
- Back-to-back user agent (B2BUA) APIs  
JSR 289 simplifies the B2BUA pattern in applications with the use of the B2BUA helper class. The B2BUA is a frequently used application pattern. The B2BUA acts as an endpoint for two or more

dialogs and forwards requests and responses between those dialogs. The B2BUA helper can create a copy of an incoming request. It also automatically maintains links between sessions on both sides of the B2BUA. For more information on B2BUAs, see section 12 of the JSR 289.

## SIP application router on Liberty

8.5.5.7

The Session Initiation Protocol (SIP) container uses the SIP application router to select the order in which applications are run within the container.

The SIP container can invoke multiple applications to deploy a complete service or function. This modular and compositional approach makes it easier for application developers to develop new applications. The modular applications can be more easily combined and managed, while individual application implementations remain independent.

The application router is responsible for selecting the correct applications in the correct order to service an incoming message. An application router is required for a container to function, but it is a separate logical entity from the container. The application router is based on the JSR 289 specification. See the specification for more details about the application router function.

The default application router (DAR) can be configured with a standard configuration file, which is supplied to the SIP container as defined in JSR 289.

Application routing, also referred to as application composition, can be handled in a number of ways:

- Configure a custom application router (CAR) by specifying the path of the Java™ archive (JAR) file that contains the application router implementation and provider to the `library` element and add the `bell` element to refer to this library in the `server.xml` file. A specific provider is defined on the `carProvider` attribute of the `sipApplicationRouter` element. For an example see the documentation for “Administering Session Initiation Protocol (SIP) on Liberty” on page 1728.
- Configure the DAR by providing its location on the `sipDarConfiguration` attribute of the `sipApplicationRouter` element in the `server.xml` file.

## Session Initiation Protocol (SIP) container on Liberty

8.5.5.7

A *SIP container* is a web application server component that invokes the Session Initiation Protocol (SIP) action servlet and that interacts with the action servlet to process SIP requests.

The servlet container provides the network services over which requests and responses are received and sent. It decides which applications to invoke and in what order. The container also contains and manages servlets through their lifecycle.

A SIP servlet container manages the network listener points on which it listens for incoming SIP traffic. A listener point is a combination of transport protocol, IP address, and port number. The SIP servlet container supports the following transport protocols:

- User Datagram Protocol (UDP)
- Transmission Control Protocol (TCP)
- Transport Layer Security (TLS) over TCP

## SIP industry standards compliance on Liberty

8.5.5.7

Session Initiation Protocol (SIP) on Liberty complies with industry standards for both the SIP container and SIP applications.

## SIP container

Liberty complies with the following SIP standards:

IETF

JCP

Liberty also complies with the Internet Engineering Task Force (IETF) and Java Community Process (JCP) industry standards for SIP. The following table contains a list of the IETF and JCP standards.

*Table 12. Liberty complies with these SIP standards*

Standard	Description
JR116	SIP: SIP Servlet API
JR289	SIP: SIP Servlet API v1.1
RFC 2543	SIP: Session Initiation Protocol
RFC 3261	SIP: Session Initiation Protocol
RFC 3262	Reliability of provisional responses in SIP
RFC 3263	Locating SIP servers
RFC 3265	SIP-specific event notification
RFC 3311	The SIP UPDATE Method
RFC 3325	Private Extensions to the SIP for asserted identity within trusted networks
RFC 3326	The Reason Header field for the SIP
RFC 3515	The SIP Refer method
RFC 3581	The SIP Extension for Symmetric Response Routing
RFC 3824	Using E.164 numbers with the SIP
RFC 3891	The SIP Replace header
RFC 3903	SIP Extension for event state publication
RFC 3911	The SIP Join header
RFC 4475	SIP torture test messages
RFC 5057	Multiple dialog usages in SIP
RFC 5626	Managing Client-Initiated Connections in SIP <b>Note:</b> The SIP server can act as a proxy or registrar as specified in sections, 5, 6, and 7 of RFC 5626. RFC 5626 is an extension to RFC 3261. The SIP server has full support for RFC 3261. However, support for RFC 5626 comes with the following limitations: <ul style="list-style-type: none"><li>• The SIP server can act as a User Agent, as defined in RFC 3261; however, it cannot act as a User Agent as defined in section 4 of RFC 5626.</li><li>• The SIP server does not support STUN keepalives, as specified in RFC 5626.</li></ul>
RFC 5658	Addressing Record-Route issues in SIP

## SIP applications

Liberty complies with standards for SIP applications.

*Table 13. Compliance with standards for SIP applications.*

Standard	Description
RFC 2848	The PINT Service Protocol: Extensions to SIP and Session Description Protocol (SDP) for internet protocol (IP) access to telephone call services
RFC 2976	The SIP INFO method

Table 13. Compliance with standards for SIP applications (continued).

Standard	Description
RFC 3050	Common gateway interface for SIP
RFC 3087	Control of service context using SIP request-URI
RFC 3264	An offer and answer model with SDP
RFC 3266	Support for IPv6 in SDP
RFC 3312	Integration of resource management and SIP
RFC 3313	Private SIP extensions for media authorization
RFC 3319	Dynamic Host Configuration Protocol (DHCPv6) options for SIP servers
RFC 3327	SIP Extension Header field for registering non-adjacent contacts
RFC 3372	SIP for telephones (SIP-T): context and architectures
RFC 3398	Integrated Services Digital Network (ISDN) User Part (ISUP) to SIP mapping
RFC 3428	SIP extension for instant messaging
RFC 3455	Private Header (P-Header) extensions to the SIP for the 3rd-Generation Partnership Project (3GPP)
RFC 3578	Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) overlap signaling to the SIP
RFC 3603	Private SIP proxy-to-proxy extensions for supporting the PacketCable distributed call signaling architecture
RFC 3608	SIP Extension Header field for service route discovery during registration
RFC 3665	SIP basic call flow examples
RFC 3666	SIP Public Switched Telephone Network (PSTN) call flows
RFC 3680	A SIP event package for registrations
RFC 3725	Best current practices for third-party call control (3pcc) in the SIP
RFC 3840	Indicating user agent capabilities in the SIP
RFC 3842	A message summary and message waiting indication event package for the SIP
RFC 3856	A presence event package for the SIP
RFC 3857	A watcher information event template package for the SIP
RFC 3959	The early session disposition type for the SIP
RFC 3960	Early media and ringing tone generation in the SIP
RFC 3976	Interworking SIP and intelligent network (IN) applications
RFC 4032	Update to the SIP preconditions framework
RFC 4092	Usage of the SDP Alternative Network Address Types (ANAT) semantics in the SIP
RFC 4117	Transcoding services invocation in the SIP using third-party call control (3pcc)
RFC 4235	An invite-initiated dialog event package for the SIP
RFC 4240	Basic network media services with SIP
RFC 4353	A framework for conferencing with the SIP
RFC 4354	A SIP event package and data format for various settings in support for the push-to-talk over cellular (PoC) service
RFC 4411	Extending the SIP Reason Header for preemption events
RFC 4457	The SIP P-user-database Private-Header (P-Header)
RFC 4458	SIP URIs for applications such as voicemail and interactive voice response (IVR)
RFC 4483	A mechanism for content indirection in SIP messages

Table 13. Compliance with standards for SIP applications (continued).

Standard	Description
RFC 4497	Interworking between the SIP and QSIG
RFC 4508	Conveying feature tags with the SIP REFER method

## Liberty: Real-Time Communications



8.5.5.7

The Liberty Real-Time Communications feature `rtcomm-1.0` enables a highly scalable signaling infrastructure that you can use to connect WebRTC clients and other types of Internet of Things (IoT) nodes into real-time audio, video, or data interactions.

The feature supports both registrations of clients, as well as the exchange of signaling that is needed to create a WebRTC peer connection between two endpoints.

WebRTC is an emerging HTML5 standard set of JavaScript APIs that enable developers to add real-time communications to their web applications by using only JavaScript with no browser plug-ins. To learn more about WebRTC go to [WebRTC](#) and to learn more about the IBM solutions for WebRTC, see [WebSphere Liberty Real-Time Communications and WebRTC](#). While WebRTC encompasses things such as audio and video codecs, echo cancellation, and Interactive Connectivity Establishment (ICE) for firewall traversal of media streams, it does not include support for the call signaling needed to set up the media streams between endpoints that want to communicate. The new `rtcomm-1.0` feature provides a call signaling connector that runs on Liberty and also includes a client-side JavaScript library that encapsulates both call signaling and a wrapper for WebRTC. The library exposes a simple API for rapid integration of audio, video, or data communications into new and existing web applications.

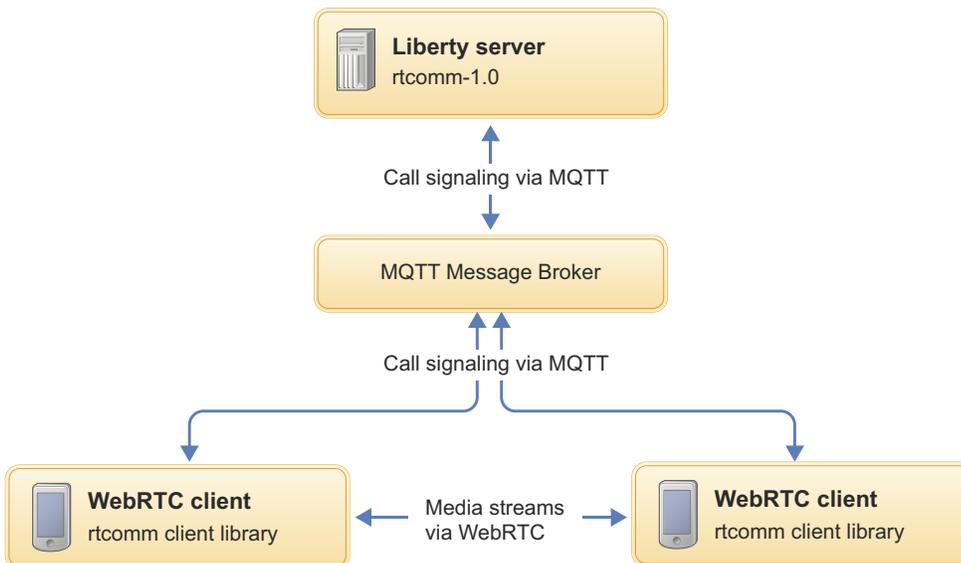


Figure 18. Components that make up the Rtcomm Feature

As the diagram shows, the WebRTC clients communicate with the backend Liberty server via the Message Queue Telemetry Transport (MQTT). MQTT is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol. This protocol is a lightweight publish and subscribe messaging transport. MQTT is an open standard and open source clients exist for JavaScript, Java, and many other languages; see [MQTT](#) for details. The `rtcomm` client library is built on top of the Eclipse Paho JavaScript client that uses `WebSocket` as its underlying transport; see [Paho](#) for details.

Many options of MQTT message brokers exist in the market today. For development purposes, IBM MessageSight for Developers can be downloaded from the following URL, IBM MessageSight for Developers. Here is a list of some of the more commonly used MQTT message brokers:

- IBM MessageSight
- WebSphere MQ Telemetry
- Mosquitto (open source MQTT broker)

**Attention:** Public, cloud-based MQTT brokers like MQTT Dashboard should not be used for anything more than testing. There is no way to predict when public servers will go up and down and many public servers periodically delete their open connections and subscriptions. Production deployments must always rely on a secure server such as a deployment of IBM MessageSight.

**Note:** Make sure that the MQTT message broker you are using supports WebSocket, otherwise, the WebRTC clients cannot connect to it.

## Configuring Liberty Real-Time Communications



8.5.5.7

Configuring the Real-Time Communications feature consists of updates to the `server.xml` file.

### About this task

To configure a Liberty server to run an application that is enabled for Real-Time Communications, you must set the `rtcomm-1.0` feature. You can also enable several other configurations and options to work with an application that is using Real-Time Communications.

**Note:** The `Rtcomm` Feature does not currently support Liberty collectives or clustering. Only a single Liberty instance per `rtcommTopicPath` is currently supported.

### Procedure

1. To enable the `rtcomm-1.0` feature after downloading the Liberty server, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<featureManager>
  <feature>rtcomm-1.0</feature>
</featureManager>
```

If you would like to modify the default settings you need to add the `Rtcomm` Feature to the Liberty server configuration. To do this, you can either use the WDT tool or manually add the following configuration line to the `server.xml` file:

```
<rtcomm/>
```

The default settings include:

- `Rtcomm` MQTT Broker Connection Details: (host: localhost and port: 1883)
- `Rtcomm` root topic path: `/rtcomm/`
- SSL is disabled

**Note:** For the default settings to work, an MQTT Broker needs to be installed and enabled on the same machine as the Liberty server.

If you would like to change the default settings for the MQTT Broker, you will need to edit the `server.xml` file with the following:

```
<rtcomm messageServerHost="<brokerhostname>" messageServerPort="<brokerportname>" />
```

2. Configure the Rtcomm topic path. The `rtcommTopicPath` is used with other Rtcomm topic names. This topic path provides a unique name space to avoid collisions with other developers that use the same message broker. To set this path, add the following configuration line to the `server.xml` file:

```
<rtcomm rtcommTopicPath="/rtcomm/" />
```

You must pass the name and path you configured into the `rtcomm` client library on initialization along with the message broker address. The server creates the topic name and appends it to the topic path.

**Note:** The `rtcommTopicPath` must be unique per the Liberty server whenever multiple Liberty servers are configured to use the same MQTT broker, otherwise there is no way to predict the behavior.

3. You can configure the shared subscription path that is prepended to the `rtcommTopicPath`. This path is required by message brokers when using shared subscriptions. To set this path, add the following configuration line to the `server.xml` file:

```
<rtcomm sharedSubscriptionPath="$SharedSubscription/rtcomm/" />
```

Shared subscriptions must be configured when using call queues. Call queues rely on shared subscriptions to distribute messages across all the queue listeners. For example, if multiple help-desk agents are all listening on a single queue, shared subscriptions are used to distribute calls to one agent at a time.

**Note:** Shared subscription support is a non-standard in MQTT brokers. The previous configuration shows how to properly setup the `rtcomm-1.0` Feature to work with IBM MessageSight. Refer to your broker's product documentation regarding configuring shared subscriptions.

4. **Optional:** Configure more options when using the Rtcomm Feature.

#### Configuring backend services with the Rtcomm Feature

The Rtcomm Feature supports a number of backend services that include the following:

- Interactive Connectivity Establishment (ICE) server configuration: Specifies URLs that are sent to and used by the Rtcomm WebRTC clients when negotiating peer media sessions.
- Call Queue support: Rtcomm can be configured to support shared call queues, and enables the user to create a shared call queue where many agents can subscribe to a specific call queue and respond to customer calls. For example, you can dial into customer support for a specific product. Many agents can subscribe to the queue, but only one agent is chosen to respond to each call.
- Rtcomm Gateway: Adds the capability for connecting Session Initiation Protocol (SIP) with Rtcomm WebRTC endpoints for the exchange of audio and video streams. For further details on configuring an Rtcomm Gateway, see [Configuring a Rtcomm Gateway](#).
- Alternate Endpoint Routing: Specifies that the user wants to route new sessions through an alternative endpoint.

#### Interactive Connectivity Establishment (ICE) Server Configuration

ICE is a technique that is used in computer networking that involves NATs (Network Address Translators) in Internet applications, such as, Voice over Internet Protocol (VoIP), peer-to-peer communications, video, instant messaging and other interactive media. In such applications, NAT traversal is an important component to facilitate communications that involve hosts on private network installations, often located behind firewalls.

The Node Controller provides ICE server configuration as a way to notify Rtcomm client nodes which ICE servers they can use when setting up peer-to-peer sessions with another client. WebRTC relies heavily on ICE servers to traverse firewalls, and being in production deployments it is critical to include support for ICE to ensure the highest possible probability for connecting endpoints.

The ICE server configuration is accessed through a service query request that is published to the connector topic name associated with a Rtcomm Feature. For more information about the Rtcomm service query, see the protocol details, [GitHub lib.rtcomm.clientjs](#).

To configure various types of ICE servers, add the following property to the `rtcomm` configuration line in your `server.xml` file:

```
<rtcomm>
  <iceServerURL>stun:example1.hostname.com:8880</iceServerURL>
  <iceServerURL>stun:example2.hostname.com:8881</iceServerURL>
</rtcomm>
```

### Third-Party Call Control

You can find all protocol details that define the message formats that are related to third-party call control in the GitHub repository. The `lib.rtcomm.node-red` and `lib.rtcomm.node` related open source components are used to interact with these services.

### Call Queue Support

Call queues provide a round robin style interaction where many users can subscribe to a queue and another user can call the queue. Only one of the subscribed users will receive the call. This feature is enabled by defining queues and enabling Shared Subscriptions as previously shown in step two.

In order to configure call queues, configure the shared subscription path that is prepended to the `rtcommTopicPath`. This path is required by message brokers when using shared subscriptions. You can define the `callQueues` that are supported by adding the following configuration lines to the `server.xml` file:

```
<rtcomm sharedSubscriptionPath="$SharedSubscription/rtcomm/">
  <callQueue description="refrigerator" callQueueID="callQueueID2" timeout="500s"></callQueue>
</rtcomm>
```

The user can create as many unique call queues as they need. When configured, the shared subscription path plus the `rtcomm` topic path plus the topic name ("`$SharedSubscription/rtcomm//rtcomm/callQueue`") is subscribed to by agents to receive call requests from the server.

The following configuration items are available for each queue:

- **Configure description:** Specifies the verbal description of this call queue instance. This verbal description is returned in service query responses and can be used to better inform the client about the queue.
- **Configure callQueueID:** The endpoint ID that is associated with the call queue topic name, and that is the destination endpoint ID that a caller uses to call into a specific queue.
- **Configure timeout:** The number of seconds to wait before terminating a call that is waiting in a queue.

### Alternate Endpoint Routing

Specifies that the user wants to route new sessions through an alternative endpoint. Using this option, you can subscribe to the `alternateEndpointRouting` topic name, such as `/rtcomm/alternateEndpointRouting` and are able to route new sessions to the proper endpoint. To enable this capability, add the following configuration line to the `server.xml` file:

```
<rtcomm alternateEndpointRoutingEnabled="true"/>
```

### SSL configuration for Rtcomm

Make sure the environment is configured to use SSL between the `Rtcomm` Feature and the MQTT broker.

The SSL reference is the ID of the SSL configuration that is used to connect to the SSL-enabled MQTT Broker.

**Note:** In order for the `Rtcomm` Feature to use SSL, the `SSL` Feature must be enabled. To enable the `SSL` Feature, add the following configuration to the `server.xml` file.

```
<rtcomm sslEnabled="true" sslRef="mySSLConfig" />
```

For further details on the `sslRef` configuration attribute, see [Liberty: SSL configuration attributes](#).

## Using the rtcomm-1.0 WebRTC JavaScript client and services



8.5.5.7

The Liberty `rtcomm-1.0` feature relies on an open signaling protocol that is used to establish real-time multimedia sessions over MQTT between Rtcomm endpoints, which support WebRTC.

Open source implementations of the `rtcomm-1.0` protocol are released on the GitHub repository and include the following:

### **lib.rtcomm.clientjs**

This GitHub repository contains a client library and sample code that uses the Rtcomm signaling protocol to simplify using WebRTC in the browser. The library is written in JavaScript and gives the application developer a simple interface to create WebRTC connections between two browsers. The library documentation, including how to install and its API, are in the GitHub repository. See GitHub `lib.rtcomm.clientjs`.

For a sample mobile application using `lib.rtcomm.clientjs`, see `sample.rtcomm.mobile`.

### **lib.angular-rtcomm**

This GitHub repository contains the Rtcomm `Angular.js` module that exposes a set of real-time communication features in the form of a service and a number of Angular directives and controllers. See `lib.angular-rtcomm`.

### **lib.rtcomm.node**

This GitHub repository contains a `node.js` module that provides service functionality to monitor events by using selective filters and initiate a third-party call between two clients. This module can be used independently or with the `lib.rtcomm.node-red` nodes in Node-RED. The module documentation, including how to install and its API are in the GitHub repository. See GitHub `lib.rtcomm.node`.

### **lib.rtcomm.node-red**

This GitHub repository contains a set of `node-red` nodes that use the `lib.rtcomm.node` module. One of the Node-RED nodes enables the consumption of `rtcomm-1.0` events in the Node-RED environment and outputs these events to other nodes using filters. This repository also includes a Node-RED node that can instantiate a third-party call that is based on inputs from other nodes. The node documentation, including how to install and its API are in the GitHub repository. See GitHub `lib.rtcomm.node-red`.

For more information about the `rtcomm-1.0` protocol, see the Rtcomm Signalling Protocol specification on GitHub. The `rtcomm-1.0` feature also provides a service interface that allows for the monitoring of Rtcomm related events and third-party call control. For more information, see the Rtcomm Service Protocol specification on GitHub. Protocol version numbers are listed in the title of these documents and define the version number for the included implementation. GitHub releases are used to tag all the repository files related to a protocol version number.

## Configuring a Rtcomm Gateway



8.5.5.7

The Rtcomm Gateway adds the capability for connecting Session Initiation Protocol (SIP) with Rtcomm WebRTC endpoints for the exchange of audio and video streams.

## About this task

The Rtcomm Gateway (GW) is useful when you require federating between the Rtcomm network and different vendors' networks. The other network can be a network of WebRTC endpoints, which is using a different method for signaling, or it can also be a different network of Voice over IP (VOIP) devices or even the Public switched telephone network (PSTN). Such federation is possible as long as the other network provides an edge GW element that supports the widely adopted SIP protocol.

The Rtcomm Gateway supports both Interactive Connectivity Establishment (ICE) for SIP (based on RFC 5245) and trickle ICE for SIP (based on the IETF draft). This draft is still marked as a “work in progress” so this implementation might change in the future in accordance to this draft progress.

## Procedure

1. Add the `rtcommGateway-1.0` feature in the `server.xml` file to enable the Rtcomm Gateway capability.

```
<featureManager>
  <feature>rtcommGateway-1.0</feature>
</featureManager>
```

The Rtcomm Gateway is configured in the `rtcomm` section. This configuration enables you to define the following:

- a. Instructs the GW on where to direct the SIP message that is translated from an incoming Rtcomm signaling message. There are three options:
    - Nothing is configured (default): The GW tries to resolve the destination based on the SIP address that was provided as the target on the Rtcomm WebRTC client.
    - `sipContainer=true`: The GW sends the message to the internal Liberty SIP servlet container port. This message gets routed to a JSR 289 application that is installed on the Liberty server, according to the standard application router rules. For further details, see Session Initiation Protocol (SIP) applications on Liberty.
    - `ExternalPR=host:port`: Tells the GW to route the translated SIP message to an external destination of a SIP Proxy or Registrar.
  - b. Define the SIP endpoint for incoming SIP messages. Messages coming on the SIP endpoint get translated to Rtcomm signaling and delivered by the GW to the WebRTC endpoint, that is resolved from the SIP initial message `requestURI` header.
2. Review the following additional considerations for implementing Rtcomm Gateway.
    - a. Sending messages from Rtcomm WebRTC to SIP.
      - REGISTER: When sending an Rtcomm register message from the WebRTC client that is using the DOCUMENT message, it is possible to use a SIP address of record (AOR) as the client topic. If such a SIP URI is registered, the GW converts that to a SIP REGISTER request and tries to route it according to the rules defined by the configuration. The Contact header is constructed from a Rtcomm Gateway SIP endpoint address, as configured for the Liberty server, and the user name as set in the AOR.
      - Rtcomm START\_SESSION message can be directed to a SIP address as well. In this case, the START\_SESSION `toEndpointID` field is populated by a URI, which starts with either of 'sip', 'sips', or 'tel' scheme prefixes, then the message is translated to a SIP INVITE and sent according to the rules configured. All subsequent messages in the dialog are translated to SIP according to the signaling scenario defined and the relevant Request For Comments (RFC). This rule applies to both the Interactive Connectivity Establishment (ICE) and trickle ICE signaling scenarios.
    - b. Sending messages from SIP to Rtcomm WebRTC.

The GW currently supports only INVITE dialogs. A SIP INVITE that is coming into one of the configured GW SIP endpoints is translated to an Rtcomm START\_SESSION message and sent to the resolved WebRTC endpoint. The WebRTC endpoint is resolved according to the following rules:

      - Look for the INVITE `requestURI` SIP address. If the endpoint was registered as a client topic by a previous Rtcomm DOCUMENT message, then this is where the START\_SESSION message is directed

to. For example; if the Rtcomm endpoint was registered as "sip:bob@x.y.z.w" as a DOCUMENT topic, then any INVITE with "sip:bob@x.y.z.w requestURI" is converted to START\_SESSION and directed to that MQTT topic.

- If the previous step did not resolve a destination, look for only the user part in the SIP requestURI. If the endpoint was registered, the START\_SESSION is directed to that topic. For example; if the Rtcomm endpoint was registered as "bob", then for any <domain> in the requestURI is bob@domain.

**Note:** Unsupported SIP requests return with a 405 error response.

c. Transcoding and advanced media server functionality.

- The Rtcomm Gateway does not support handling the media plane and will not perform actions such as transcoding between SIP V0IP and WebRTC endpoints codecs. This means that at its basic use, the GW allows only federation between different WebRTC endpoints, or endpoints that use similar codecs and streaming protocols, such as the WebRTC standard.
- To make full use of the Rtcomm Gateway capabilities, it is possible to augment the Liberty server with a feature that provides APIs for a media server connector based on the JSR 309 standard. With this feature, you can create and install an application on the Liberty server that uses a media server for transcoding and streaming protocol translation, in addition to many other advanced features such as recording, announcements playback, stream mixing for multi-party A/V conferences and many more. Details can be found in the JSR 309 specification.
- See WASdev to find a sample application that uses JSR 289 and 309 to connect a SIP soft phone and the Rtcomm WebRTC endpoint using a media server as a mediator and translator for the media.
- The application is using SIP Servlets (JSR 289) with JSR 309 and mediates between the SIP network and the Rtcomm WebRTC network. This application only requires the configuration of internal routing in the server.xml file; for example:

```
<rtcomm messageServerHost="<brokerhostname>" messageServerPort="<brokerhostport>"
      <gateway sipContainer="true"></gateway>
</rtcomm>
```

**Note:** Make sure that the SIP ports where incoming SIP messages are directed to are those of the SIP Servlets container endpoints and not the GW endpoint. See Administering Session Initiation Protocol (SIP) on Liberty.

## Example

In this example, the incoming WebRTC messages are directed to an external SIP endpoint that might be a proxy or registrar, such as 1.2.23.2:5063.

```
<rtcomm messageServerHost="<brokerhostname>" messageServerPort="<brokerhostport>"
      <gateway sipContainer="false" externalPR="1.2.23.2:5063" allowFromSipEndpointRef="webrtc2, webrtc"></gateway>
</rtcomm>
```

Incoming SIP messages can be on the "webrtc" and "webrtc2" SIP endpoints. In the following example, "webrtc" is using the default ports that are 5060 and localhost.

```
<sipEndpoint id="webrtc"></sipEndpoint>
<sipEndpoint id="webrtc2" sipTCPport="5067" sipUDPport="5067" sipTLSport="5068" host="*"></sipEndpoint>
```

## Configuring Security for the rtcomm-1.0 Feature



8.5.5.7

This topic describes the many aspects of securing the rtcomm-1.0 Feature.

## About this task

The following steps describe how to enable security for the rtcomm-1.0 Feature.

### Procedure

1. Configure SSL.

#### SSL between the rtcomm-1.0 Feature and the MQTT Broker

This function is enabled for the rtcomm-1.0 Feature by setting the `sslEnabled="true"` attribute for `Rtcomm` in the `server.xml` file, and this often requires a different port for SSL (default 8883) to connect to the broker.

#### SSL between the Rtcomm JavaScript Client and the MQTT Broker

If the `rtcomm.js` client is served over `https`, then it will enable SSL by default (and will try to use port 8883) otherwise SSL needs to be enabled in the configuration when initializing the `EndpointProvider`. The configuration resembles the following:

```
var providerConfig = {
    server: mqttbroker server,
    port: mqttbroker SSL Port,
    useSSL: true};
```

The previous steps ensure that the communication between the clients, the MQTT Broker, and the Liberty server that is running the rtcomm-1.0 Feature is encrypted.

2. Configure authentication.

#### Authentication and Authorization of the JavaScript Client with the MQTT Broker

Typically, an application that is implementing Real-Time Communications authenticates a user. For further details, see [Authenticating users in Liberty](#).

Many external MQTT Brokers can require authentication but will not use the same authentication as the application without a specific configuration.

An external MQTT Broker can use similar authentication mechanisms and offer ways to use LTPA Tokens to verify identity. IBM MessageSight supports LTPA and when the LTPA Keys are shared with the MessageSight MQTT Broker they are members of the same domain (`servername.domainname.com`), and they both are using the same LDAP resource for identifying users, then an LTPA Token can be used to pass the original authentication to IBM MessageSight. Other MQTT Brokers can work similarly. For further details on using LTPA with IBM MessageSight, see [Lightweight Third Party Authentication \(LTPA\)](#).

The Liberty server must be configured by using the following information, [Configuring LTPA in Liberty](#).

**Note:** Use the `ssoDomainNames` attribute to define the common domain between servers:

```
<webAppSecurity logoutOnHttpSessionExpire="true" singleSignonEnabled="true" ssoDomainNames="domainname.com" />
```

Authentication that uses LTPA is separate from authorization or authorization in IBM MessageSight, and it is necessary to follow the directions at this [URL](#), [Authorization](#).

This configuration only works if the original authenticator that is providing the LTPA token and the MessageSight server share the same LDAP configuration.

#### Client authentication without LTPA

If LTPA cannot be configured, the `rtcomm.js` client provides an API that allows a user and password to be provided for authentication with the MQTT Broker, and is done in the configuration that is passed to the `EndpointProvider` during the `init()`:

```
var providerConfig = {
    server: servername,
    port: port,
    useSSL: true,
```

```
credentials: {
  username: "username",
  password: "password" }
};
```

This configuration passes the identity and password to the MQTT client to authenticate the connection to the MQTT Broker.

## Configuring the Media Server Control Feature

8.5.5.8

JSR 309 (Media Server Control) controls Media Resource Functions (MRFs) which are server-side media processing servers.

### About this task

The Liberty Media Server Control feature (`mediaServerControl-1.0`) enables the ability to access media servers through the JSR 309 API. For applications to use this API, a driver implementation of JSR 309 must be installed. For more information about JSR 309, see JSR 309: Media Server Control API.

### Procedure

To enable the `mediaServerControl-1.0` feature, add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<featureManager>
  <feature>mediaServerControl-1.0</feature>
</featureManager>
```

---

## Multimedia

Watch videos, webcasts, and other media about Liberty.

If you do not find the media you want in this topic, see the following websites for media about Liberty and IBM WebSphere Application Server products:

- IBM SupportTV YouTube channel
- WebSphere Application Server YouTube playlists
- IBM Education Assistant for WebSphere Application Server

### Overview

-  [Why Liberty? Performance that scales \(V8.5.5.6\) \[Transcript\]](#)
-  [Why Liberty? Fast application development \(V8.5.5.6\) \[Transcript\]](#)
-  [Why Liberty? Rapid deployment and powerful administration \(V8.5.5.6\) \[Transcript\]](#)
-  [Java EE 7 in Liberty \(V8.5.5.6\) \[Transcript\]](#)
-  [Thoughts on Liberty: Interview with Alasdair Nottingham \(V8.5.5\) \[Transcript\]](#)
-  [WebSphere Application Server V8.5.5 release overview \(V8.5.5\)](#)

### Installing and getting started

-  [Installing Liberty from a ZIP file \(V8.5.5.6\) \[Transcript\]](#)
-  [Enabling IHS for Liberty Dynamic Routing \(V8.5.5.4\) \[Transcript\]](#)
-  [Using the Liberty Repository to enhance Liberty environments \(V8.5.5.2\) \[Transcript\]](#)
-  [Installing WebSphere eXtreme Scale with Liberty \(eXtreme Scale V8.6.0.5\) \[Transcript\]](#)

## Setting up and configuring

-  Configure session cache management with Liberty and WebSphere eXtreme Scale (InterConnect 2015 and eXtreme Scale V8.6.0.6) [Transcript]
-  Setting up Admin Center (V8.5.5.4) [Transcript]
-  Comparing collectives and cells (V8.5.5) [Transcript]
-  Introduction to creating a Liberty collective (V8.5.5) [Transcript]
-  Configuring a Liberty auto-scalable cluster for JVM elasticity (V8.5.5.4) [Transcript]
-  Health management for Liberty collectives (V8.5.5.8) [Transcript]

## Administering

-  Touring Admin Center (V8.5.5.7) [Transcript]
-  Getting started with the Server Configuration Tool for WebSphere Liberty (V8.5.5.8) [Transcript]

## Securing

-  OpenID Connect on Liberty (InterConnect 2015) [Transcript]
-  Google OpenID Connect for applications on WebSphere Liberty (InterConnect 2015) [Transcript]

## Developing applications

-  Creating a Hello World Java application (V8.5.5.2) [Transcript]
-  Introduction to WebSphere Application Server Patterns 1.0 [Transcript]

## End-to-end scenarios

- Develop, build, and deploy an application with Liberty server DevOps and some open-source tools.
  -  Demo - DevOps with WebSphere Liberty Server (InterConnect 2015) [Transcript]
- Enable highly available clusters with Liberty collectives.
  1. Configure a collective controller.
  2. Join a server to the collective controller as a member server.
  3. Set up dynamic auto-scalable cluster members with JVM elasticity. The scaling controller can start or stop cluster members based on resource use and scaling policies.
  4. Enhance the dynamic auto-scalable cluster members with Liberty elasticity. Enable the scaling controller to also install Liberty software onto a registered host and create a new server.
    -  Configuring an auto-scalable cluster for Liberty elasticity (V8.5.5.7) [Transcript]

## Video: Comparing collectives and cells

The following transcript is for the “Comparing collectives and cells” video, which describes the similarities and differences between WebSphere Application Server traditional cells and Liberty collectives. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content shown in the video.

-  Comparing collectives and cells

Table 14. Demo creating a Liberty collective. Show commands and server.xml changes.

Scene	Audio	Onscreen Action
1	<p>Hi, I'm Mike Thompson. I'm going to take you today through a comparison between the WebSphere Liberty administrative domain and the WebSphere traditional administrative domain.</p> <p>The first difference is the terminology. The administrative domain in Liberty is called a <i>collective</i>, which is in comparison to the traditional administrative domain known as a <i>cell</i>.</p>	Show the developer talking on camera.
2	<p>Another key difference in terminology is the name given to the administrative server. In a cell environment, the administrative server is called a <i>deployment manager</i>, or "Dmgr" for short. In the collective, the administrative server is called the <i>collective controller</i>, or "controller" for short.</p>	<p>Show lists that compare a deployment manager (Dmgr) to a collective controller:</p> <p>Admin server: Deployment Manager (Dmgr)</p> <ul style="list-style-type: none"> <li>- Dedicated process</li> <li>Federation (tightly coupled)</li> <li>Agents</li> <li>Centralized config control</li> <li>- Dmgr owns all configuration</li> <li>Single administrative server</li> <li>Management API</li> <li>- MBean &amp; wsadmin</li> <li>- wsadmin scripting (via jython/jacl)</li> </ul> <p>Admin server: Collective Controller</p> <ul style="list-style-type: none"> <li>- Liberty feature</li> <li>Join (loosely coupled)</li> <li>Agentless</li> <li>Decentralized config control</li> <li>- Each server owns its configuration</li> <li>Highly available administrative server</li> <li>Management API</li> <li>- MBean, no wsadmin</li> <li>- jython scripting</li> </ul>
3	<p>There is an important difference between these two processes. In the cell, the Dmgr is a dedicated process, which means it is unable to run an end user workload. In the collective, the controller is actually enabled as a Liberty feature, which means that it can be enabled with any other Liberty feature, allowing the controller to run end user workloads.</p>	<p>Show lists that compare a deployment manager (Dmgr) to a collective controller and highlight:</p> <ul style="list-style-type: none"> <li>- Dedicated process</li> <li>- Liberty feature</li> </ul>
4	<p>There is also a difference in the way entities become part of the administrative domain. In the cell, the process is known as <i>federation</i>. It is a tightly coupled process whereby servers federate into the cell and give up a lot of their autonomy. In the collective, servers join the collective and become collective members. The process of joining is very lightweight and allows the members to be loosely coupled to the collective so that members can join collectives and leave collectives very easily.</p>	<p>Show lists that compare a deployment manager (Dmgr) to a collective controller and highlight:</p> <ul style="list-style-type: none"> <li>Federation (tightly coupled)</li> <li>Join (loosely coupled)</li> </ul>

Table 14. Demo creating a Liberty collective (continued). Show commands and server.xml changes.

Scene	Audio	Onscreen Action
5	The cell environment uses agents to facilitate management activities. The node agent process acts as a middleman between the deployment manager and the targets of management, the application servers. In the collective environment, there are no administrative agents. It is a completely agentless model. When a collective controller takes actions against a target member, it's taking those actions directly.	Show lists that compare a deployment manager (Dmgr) to a collective controller and highlight: Agents Agentless
6	Another key distinction between cells and collectives is the way the configuration is controlled. In the cell, the deployment manager owns all configuration of all the entities within the cell. In the collective, each server owns its own configuration. So, even when members join and leave the collective, they retain complete control over their configuration.	Show lists that compare a deployment manager (Dmgr) to a collective controller and highlight: Centralized config control - Dmgr owns all configuration Decentralized config control - Each server owns its configuration
7	The administrative server for a cell is a singleton. There is only one instance of a deployment manager active at any given time within a cell. We've recognized the need for the administrative environment to become more robust and resilient. As such, the collective controller was designed with high availability in mind, and multiple collective controllers can be running concurrently within the same collective.	Show lists that compare a deployment manager (Dmgr) to a collective controller and highlight: Single administrative server Highly available administrative server
8	Lastly, there's a difference between the management API of a cell and a collective. Both the cell and collective provide MBeans to provide management activities but only a cell provides wsadmin. The collective environment does not support wsadmin. It a design principle that the collective's management activities be exposed only via MBeans. While the cell exposes its wsadmin scripting via Jacl and Jython, the collective currently only supports Jython scripting. However, additional languages are possible.	Show lists that compare a deployment manager (Dmgr) to a collective controller and highlight: Management API - MBean & wsadmin - wsadmin scripting (via jython/jacl) Management API - MBean, no wsadmin - jython scripting

For more information, see “Liberty: Collective architecture” on page 1450 and “Configuring a Liberty collective” on page 1136.

## Video: Configure session cache management with Liberty and WebSphere eXtreme Scale

8.5.5.5

The following transcript is for the “Configure session cache management with Liberty and WebSphere eXtreme Scale” video, which describes how to improve the performance of your applications by off loading your current application server and data access processes to an in-memory cache using session cache management with Liberty and WebSphere eXtreme Scale. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content shown in the video.

 Configure session cache management with Liberty and WebSphere eXtreme Scale

Table 15. Introduction. Describe the benefits of session management with Liberty and WebSphere eXtreme Scale.

Scene	Audio	Onscreen Action
1	<p>Caching sessions in your applications is one of the most beneficial and easy-to-do configurations to improve performance and availability of your web applications. If you have an application server, store your information in sessions, then can offload your current process to an in-memory cache to help your applications run at super fast speeds. This video will help you do that by demonstrating how to set up session management quickly and simply with Liberty and WebSphere eXtreme Scale.</p> <p>Liberty is a fast, lightweight and simple Java web application container that application developers can use to develop, test and deploy applications easily.</p>	<p>Show the video title, "HTTP Session Failover for WebSphere Liberty leveraging WebSphere eXtreme Scale".</p>
2	<p>WebSphere eXtreme Scale provides distributed in-memory data storage that is replicated across different machines.</p>	<p>Show IBM Corporation notices and disclaimers.</p>
3	<p>This video includes an overview of session caching with eXtreme Scale. It also includes quick steps to download the Liberty and WebSphere eXtreme Scale for developers. You will also learn how to configure WebSphere eXtreme Scale in Liberty. And finally, a sample web application is included that demonstrates HTTP session failover to an in-memory datagrid that is hosted by WebSphere eXtreme Scale.</p>	<p>List video contents:</p> <p>Show Quick Demo, Set-Up, and Sample of Liberty with WXS</p> <p>Overview of Session and Data Caching in WXS</p> <p>Quick Steps to Download Liberty &amp; WXS</p> <p>How to Configure WXS in Liberty</p> <p>Sample Web Application demonstrating HTTP Session Failover to an In-</p>

Table 15. Introduction (continued). Describe the benefits of session management with Liberty and WebSphere eXtreme Scale.

Scene	Audio	Onscreen Action
4	<p>Why is HTTP Session Persistence important? Without HTTP session persistence, you will lose the session data if an application instance fails or becomes unresponsive. For example, in a retail scenario where a user adds items to a shopping cart, that user will most likely have to log in again and rebuild their shopping list if the application fails and session failover is not enabled. Usually that experience creates an unhappy customer.</p> <p>Developers have 3 options to persist HTTP session data:</p> <p>First option: Developers can store sessions locally in the application server memory space, but other application server instances will not share the common user session for web applications. If the instance fails, the session is lost and the user experience is less than desirable.</p> <p>Second option: Developers can persist sessions in a relational database that is shared among instances, but the architecture of relational databases have inherent scalability concerns and reading or writing to a disk is slower than on an in-memory data grid.</p> <p>The third and best option is what this video highlights, where Liberty uses a shared persistence engine to store HTTP session data in the memory of an elastic, scalable architecture, which is known as WebSphere eXtreme Scale. Using Liberty with WebSphere eXtreme Scale allows two or more independent Liberty instances to share a common user session for web applications. When one instance fails, the remaining instances can continue to serve user requests as if no failure had occurred.</p> <p>If maintaining HTTP session high availability is a priority, then use WebSphere eXtreme Scale. Even if a runtime instance fails, the customer session is maintained. The customer is unaware of the failure or maintenance activity, which allows a consistent customer experience without interruption or data loss.</p>	<p>Show information about HTTP session failover: Hands-On Demo: Session Cache HTTP Session Failover for Liberty</p> <p>Customer has an enterprise web application on Liberty, but they w</p>

Table 15. Introduction (continued). Describe the benefits of session management with Liberty and WebSphere eXtreme Scale.

Scene	Audio	Onscreen Action
5	<p>Using WebSphere eXtreme Scale with Liberty offers several benefits to developers:</p> <ul style="list-style-type: none"> <li>• Distributed data access for high availability</li> <li>• In-memory access with rapid retrieval</li> <li>• Scalability built in over traditional methods like relational databases or memory-to-memory session replication</li> <li>• Remote access to eliminate single points of failure</li> <li>• The benefit of a quick configuration in a Liberty environment</li> </ul>	<p>Show information about Liberty data caching: Liberty Data Caching with WXS</p> <p>Supports distributed caching scenarios for web and mobile applications.</p> <p>Store key and value objects in memory for fast access.</p> <p>Provides linear scalability, predictable performance, and fault tolerance. Replicates data so that cache components may be restarted without data loss.</p> <p>Caching is an example of a composable element that can be used to build...</p>

Table 16. Demo installing Liberty and WebSphere eXtreme Scale for Developers Liberty. Show commands and server.xml changes.

Scene	Audio	Onscreen Action
6	<p>To experience this capability, you can quickly install Liberty and WebSphere eXtreme Scale for Developers Liberty on your development machine:</p> <ol style="list-style-type: none"> <li>1. Go to WASdev.net.</li> <li>2. Download Liberty.</li> <li>3. Download WebSphere eXtreme Scale for Developers Liberty.</li> <li>4. Install the JAR files into the "hands on" directory, which is the example directory for this demo.</li> </ol>	<p>Show the steps:</p> <ol style="list-style-type: none"> <li>1. Go to the WASdev website.</li> <li>2. Select <b>Want to try the Beta?</b></li> <li>3. From <b>Liberty Repository</b>, select <b>WebSphere eXtreme Scale for Developers Liberty</b>.</li> <li>4. Install the JAR files in my c:\hands-on&gt; directory.</li> </ol>
7	<p>To demonstrate the capabilities of WebSphere eXtreme Scale as a shared, remote HTTP session data grid, you will see a sample application (from the displayed URL) that is deployed locally in the dropin directory of the Liberty web instances, which shows you some examples of placing and retrieving session objects to a data grid.</p>	<p>Show illustrations of the WebSphere eXtreme Scale HTTP session sample and the http://ibm.co/1umQ7iy URL.</p>
8	<p>You will learn how to configure Liberty instances to act as two Liberty web instances that are clients to a WebSphere eXtreme Scale data grid.</p> <p>You will set up a WebSphere eXtreme Scale server as a HTTP session store running on a separate Liberty JVM.</p> <p>And finally, you will configure the two Liberty web instances to store HTTP session data in the data grid of a WebSphere eXtreme Scale container.</p>	<p>Show information about HTTP session failover: Hands-On Demo: Session Cache</p> <p>HTTP Session Failover for Liberty</p> <p>Customer has an enterprise web application on Liberty, but they want...</p> <p>A graphic shows ServerA and ServerB in Liberty connected to a session cache.</p>

Table 17. Demo configuring Liberty to connect to the data grid. Show server configuration and testing in a browser.

Scene	Audio	Onscreen Action
9	<p>Now, you will learn to configure Liberty to connect to the data grid. By installing WebSphere eXtreme Scale with Liberty, you get access to features that you can use to manage HTTP session applications that are installed in Liberty.</p> <p>For the remote WXS_Session_Server Liberty instance, the server feature will be set. The server feature contains the capability for running an eXtreme Scale server, which means that both the eXtreme Scale catalog and container are running. Add the server feature when you want to run a catalog server in Liberty or when you want to deploy a data grid application into Liberty.</p> <p>The webGrid feature is to host a session management data grid in the WXS_Session_Server Liberty instance. A Liberty server can host a data grid that caches and then replicates HTTP session data for fault tolerance of applications.</p> <p>Use the webApp feature to enable session management for ServerA and ServerB Liberty instances. The webApp feature contains the capability to extend the Liberty application. Add the webApp feature when you want to replicate HTTP session data for fault tolerance. Remember to set the catalogHostPort to the host and port of the WXS_Session Server Liberty instance.</p>	<p>Show information about configuring a Liberty server.xml to run WXS:</p> <p>The server feature contains the capability for running an eXtreme Scale server, both catalog and container.</p> <pre data-bbox="850 405 1349 457">&lt;feature&gt;eXtremeScale.server-1.1&lt;/feature&gt; &lt;xsServer isCatalog="true"/&gt;</pre> <p>A Liberty server can host a data grid that caches data for applications to replicate HTTP session data for fault tolerance.</p> <pre data-bbox="850 579 1360 611">&lt;feature&gt;eXtremeScale.webGrid-1.1&lt;/feature&gt; &lt;xsWebGrid objectGridName="session" catalogHostPort="remoteHost:2600"&gt;</pre> <p>The webApp feature contains the capability to extend the Liberty web application. Add the webApp feature when you want to replicate HTTP session data for fault tolerance.</p> <pre data-bbox="850 785 1349 858">&lt;feature&gt;eXtremeScale.webApp-1.1&lt;/feature&gt; &lt;httpSession idReuse="true"/&gt; &lt;xsWebGrid objectGridName="session" catalogHostPort="localhost:2600"&gt;</pre>
10	<p>The Session Sample Application is now launched on both ServerA and ServerB instances.</p> <p>Now check that the session attribute in ServerA named Loc is empty.</p> <p>Also check that the same attribute for ServerB is empty as well.</p>	<p>Show a browser open on localhost:9080/ HttpSessionWAR/ and a browser open on localhost:9081/HttpSessionWAR/. Both browsers display the WebSphere eXtreme Scale Http Session Sample with no attribute values set.</p> <p>In the browser open on localhost:9080/ HttpSessionWAR/, show typing Loc for <b>Attribute</b> in <b>Getting an attribute</b> and clicking <b>Get Attribute</b>. The browser displays <b>Welcome back. Session attribute retrieved.</b> with the Loc attribute set to null. Then show clicking <b>Main Page</b> to return to the previous page.</p> <p>Show these same steps repeated in the browser open on localhost:9081/HttpSessionWAR/.</p>

Table 17. Demo configuring Liberty to connect to the data grid (continued). Show server configuration and testing in a browser.

Scene	Audio	Onscreen Action
11	<p>Now, specify NC as the value for the Loc session attribute in the data grid through Server A's application, and verify that it was set.</p> <p>Now let's go to the ServerB Session Application and retrieve the Session attribute Loc from the data grid.</p>	<p>In the browser open on localhost:9080/ HttpSessionWAR/, show typing Loc for <b>Attribute</b> and NC for <b>Value</b> in <b>Setting an attribute</b> and clicking <b>Set Attribute</b>. The browser displays <b>Welcome back. Session attribute set.</b> with the Loc attribute set to NC. Then show clicking <b>Main Page</b> to return to the previous page. Finally, show clicking <b>Get Attribute</b> and show that the Loc attribute is set to NC, and show clicking <b>Main Page</b> to return to the previous page.</p> <p>Show in the browser open on localhost:9081/ HttpSessionWAR/ clicking <b>Get Attribute</b> and show that the Loc attribute is set to NC. Then show clicking <b>Main Page</b> to return to the previous page.</p>
12	<p>Now you can test this configuration with a simulated, unplanned outage on ServerA by stopping the Liberty instance for ServerA and verifying that ServerB can still retrieve the Loc session attribute from the session cache of the data grid.</p>	<p>Show information about HTTP session failover: Hands-On Demo: Session Cache</p> <p>HTTP Session Failover for Liberty</p> <p>Demonstration of Server failure but Customer Experience is maintained</p> <p>A graphic shows ServerA and ServerB in Liberty. ServerA is crossed out and ServerB is connected to a session cache.</p>
13	<p>ServerA is still running. But the Server A Liberty Instance will be manually stopped using the command line.</p> <p>Now let's go to the browser that was hosting ServerA Session and refresh to show the unavailable Liberty instance.</p>	<p>Show the browser open on localhost:9080/ HttpSessionWAR/. Also show entering a command to stop ServerA at a command line at C:\hands-in\wlp\bin: server stop ServerA</p> <p>Show refreshing the browser open on localhost:9080/HttpSessionWAR/. The message This webpage is not available displays.</p>
14	<p>Now that Server A is down you can verify that ServerB can still detect the Session data in the data grid. To do so, change the Loc session attribute to the value, MD.</p>	<p>Show the browser open on localhost:9081/ HttpSessionWAR/ clicking <b>Get Attribute</b> and show that the Loc attribute is set to NC. Then show clicking <b>Main Page</b> to return to the previous page.</p> <p>Show typing Loc for <b>Attribute</b> and MD for <b>Value</b> in <b>Setting an attribute</b> and clicking <b>Set Attribute</b>. The browser displays <b>Welcome back. Session attribute set.</b> with the Loc attribute set to MD. Then show clicking <b>Main Page</b> to return to the previous page. Finally, show clicking <b>Get Attribute</b> and show that the Loc attribute is set to MD, and show clicking <b>Main Page</b> to return to the previous page.</p>

Table 17. Demo configuring Liberty to connect to the data grid (continued). Show server configuration and testing in a browser.

Scene	Audio	Onscreen Action
15	<p>Now you can simulate ServerA coming back online with the ability to retrieve the new Session value, MD, for attribute Loc, which was just set through ServerB.</p> <p>Now, the browser has been refreshed and points to Server A, where the value for the Loc attribute from the data grid is retrieved.</p>	<p>Show the browser open on localhost:9081/HttpSessionWAR/. Also show entering a command to start ServerA at a command line at C:\hands-in\wlp\bin:</p> <pre>server start ServerA</pre> <p>Show refreshing the browser open on localhost:9080/HttpSessionWAR/. The browser displays the WebSphere eXtreme Scale Http Session Sample with no attribute values set.</p> <p>Finally, show clicking <b>Get Attribute</b> for the Loc attribute to show that it is set to MD, and show clicking <b>Main Page</b> to return to the previous page.</p>

Table 18. Conclusion. Summarize the video content and point viewers to more information.

Scene	Audio	Onscreen Action
16	<p>Congratulations. You've just created your first Liberty cluster with two instances pointing to a shared in-memory data grid for HTTP session storage.</p>	<p>Show information about HTTP session failover:</p> <p>Hands-On Demo: Session Cache</p> <p>HTTP Session Failover for Liberty</p> <p>Demonstration of Server Recovery or additional Liberty Instances</p> <p>A graphic shows ServerA and ServerB in Liberty with both servers connected to a session cache.</p>
17	<p>In this video, you learned the benefits of using a cache for session persistence.</p> <p>No code changes are need to the application to leverage the WebSphere eXtreme Scale data grid.</p> <p>Data for each session persists even with a server outage.</p> <p>And WebSphere eXtreme Scale is scalable up to terabytes of data and can replicate data to thousands of nodes for fault tolerance and high availability.</p>	<p>Show information about Liberty session management:</p> <p>Liberty Session Management with WXS</p> <p>Special purpose elastic in memory cache for storing HTTP session</p> <p>Stores and persists HTTP session objects to the data grid so that</p> <p>No code change to applications using the J2EE standard HTTP sessi</p> <p>Data for each HTTP session survives on a server outage for an app</p> <p>Requires no developer effort to manage</p> <p>Replicates the session data to avoid a single point of failure.</p> <p>Provides low latency data access, transactional semantics.</p>
18	<p>Visit these resources to download and install WebSphere eXtreme Scale on Liberty and to access the sample application that was used in this demo.</p> <p>Thank you for watching and this concludes the video for configuring session cache management with Liberty and WebSphere eXtreme Scale.</p>	<p>Shows resources:</p> <p>(WASdev) <a href="https://developer.ibm.com/wasdev">https://developer.ibm.com/wasdev</a></p> <p>(How to install WXS with Liberty) <a href="http://youtu.be/Zu4Z1GLJM1E">http://youtu.be/Zu4Z1GLJM1E</a></p> <p>(Sample Application used in Demo) <a href="http://ibm.co/1umQ7iy">http://ibm.co/1umQ7iy</a></p>

## Video: Configuring a Liberty auto-scalable cluster for JVM elasticity

The following transcript is for the “Configuring a Liberty auto-scalable cluster for JVM elasticity” video, which demonstrates how to configure a collective to support Java virtual machine (JVM) elasticity. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content shown in the video.

 Configuring a Liberty auto-scalable cluster for JVM elasticity

*Table 19. Title page.* Show title and then animation that illustrates autonomic starting and stopping of servers based on resource use.

Scene	Audio	Onscreen Action
1	This video shows how to configure a Liberty collective to support Java virtual machine (or JVM) elasticity.	Show title <i>Configuring a Liberty auto-scalable cluster for JVM elasticity</i> .
2	With JVM elasticity, a Liberty scaling controller can start or stop cluster members based on resource use. When resource use goes up, the scaling controller starts cluster members. When resource use goes down, the scaling controller stops cluster members. The IBM Java development kits (or JDKs) on the computers that host the cluster members provide the data on resource use.	Show animation of scaling controller stopping and starting cluster member servers. When resource use goes up, the scaling controller starts member servers. When resource use goes down, the scaling controller stops member servers.

*Table 20. Demo configuring the scaling controller.* Show adding the scalingController-1.0 feature to the server.xml file of a collective controller.

Scene	Audio	Onscreen Action
3	To set up an auto-scalable cluster, you need at least one collective controller with at least two member servers joined to the controller. I have a collective controller with three member servers.  What you see here is my collective controller and member servers in the Explore tool of the Liberty Admin Center.  You also can see the server.xml file of the collective controller. I added the adminCenter-1.0 feature to the server.xml to view the collective's servers in Admin Center.	Show the four servers in the Explore tool of Admin Center.  Also show an editor open on the server.xml file of the collective controller, which has: <pre>&lt;featureManager&gt;   &lt;feature&gt;jsp-2.2&lt;/feature&gt;   &lt;feature&gt;adminCenter-1.0&lt;/feature&gt; &lt;/featureManager&gt;</pre>
4	To make my collective controller a scaling controller, I add the scalingController-1.0 feature to its server.xml file. You can add the scalingController-1.0 feature to either feature manager. My preference is to add it below the collectiveController-1.0 feature.  Save the file.	In the editor open on the controller server.xml file, add the scalingController-1.0 feature to a feature manager: <pre>&lt;featureManager&gt;   &lt;feature&gt;collectiveController-1.0&lt;/feature&gt;   &lt;feature&gt;scalingController-1.0&lt;/feature&gt; &lt;/featureManager&gt;</pre> Then, save the file.
5	After adding the feature, I want to ensure the scaling controller feature is installed and activated. Before I enable auto scaling for the members, I want to see the message This server is elected to be the primary scaling controller in the controller's message log.	Open an editor on the controller messages.log file and scroll to the end of the log.

Table 20. Demo configuring the scaling controller (continued). Show adding the scalingController-1.0 feature to the server.xml file of a collective controller.

Scene	Audio	Onscreen Action
6	myController is now the primary scaling controller so I can enable its members to be dynamic cluster members.	In the controller messages.log file, highlight the message: CWWKV0102I: This server is elected to be the primary scaling cont

Table 21. Demo configuring a member server for auto scaling. Show adding the clusterMember-1.0 and scalingMember-1.0 features to the server.xml file of a collective member.

Scene	Audio	Onscreen Action
7	To make a collective member a <i>dynamic cluster member</i> , I add the clusterMember-1.0 feature and the scalingMember-1.0 feature to a feature manager of the collective member. I can add the features below the jsp-2.2 feature or below the collectiveMember-1.0 feature. I am adding the features below the collectiveMember-1.0 feature.	In an editor open on the server.xml file of the myMember collective member, add the clusterMember-1.0 and scalingMember-1.0 features to a feature manager: <pre>&lt;featureManager&gt;   &lt;feature&gt;collectiveMember.0&lt;/feature&gt;   &lt;feature&gt;clusterMember-1.0&lt;/feature&gt;   &lt;feature&gt;scalingMember-1.0&lt;/feature&gt; &lt;/featureManager&gt;</pre>
8	I also add a hostSingleton element to the server.xml file. I specify a hostSingleton name of ScalingMemberSingletonService and a port number of 5164. You can specify any port number, but the port number must be unique on the host computer.  All scaling members on the same host must use the same hostSingleton port.	In the editor open on the myMember server.xml file, add the hostSingleton element: <pre>&lt;hostSingleton name="ScalingMemberSingletonService" port="5164" /&gt;</pre>
9	I save the file.  For the scaling controller to recognize these changes to a member configuration, the member must be running.	Save the myMember server.xml file.  The auto scaling icon displays on the myMember card in the Explore tool.
10	To make sure that the scaling member feature is activated, I look at the member messages.  The messages show that the scaling member feature is activated, ScalingMemberSingletonService is elected the host leader, and the messenger connection goes to my scaling controller.	Open an editor on the myMember messages.log file and highlight the messages: CWWKV0200I: The ScalingMember feature is activated. ... CWWKV0203I: Server host=wasid.raleigh.ibm.com; userdir=C:/wlp/usr

Table 21. Demo configuring a member server for auto scaling (continued). Show adding the clusterMember-1.0 and scalingMember-1.0 features to the server.xml file of a collective member.

Scene	Audio	Onscreen Action
11	<p>I now copy the changes that I've made to myMember's server.xml file and make similar changes to the server.xml files of the other collective members.</p> <p>Notice that after I save the changes, an auto scaling icon displays on the member cards in the Explore tool.</p>	<p>In the editor open on the myMember server.xml file, copy the following elements:</p> <pre>&lt;featureManager&gt;   &lt;feature&gt;collectiveMember.0&lt;/feature&gt;   &lt;feature&gt;clusterMember-1.0&lt;/feature&gt;   &lt;feature&gt;scalingMember-1.0&lt;/feature&gt; &lt;/featureManager&gt;</pre> <p>&lt;hostSingleton name="ScalingMemberSingletonService" port="5164" /&gt;</p> <p>Then, highlight the second feature manager in the myMember2 server.xml file:</p> <pre>&lt;featureManager&gt;   &lt;feature&gt;collectiveMember.0&lt;/feature&gt; &lt;/featureManager&gt;</pre> <p>Paste the copied elements into the file, and save the changes.</p> <p>The auto scaling icon displays on the myMember2 card in the Explore tool. Position the cursor over the auto scaling icon on the myMember and MyMember2 cards.</p> <p>Repeat this scene for myMember3.</p>
12	<p>Because I did not specify a cluster name, the dynamic cluster members are added to the defaultCluster.</p> <p>I now have three dynamic cluster members joined to my scaling controller.</p>	<p>The name of the cluster, defaultCluster, displays on the member cards in the Explore tool.</p>

Table 22. Demo changing a default scaling policy. Mention the default scaling policies and demo changing a scaling policy.

Scene	Audio	Onscreen Action
13	<p>One of the default scaling policies requires that at least two dynamic cluster members be running.</p> <p>The other default scaling policies control when a dynamic cluster member is started or stopped. A member is started when the average members' resource use exceeds 90%. And a member is stopped when the average resource use is less than 30%.</p> <p>I'm going to change the first default scaling policy to require that only one to two dynamic cluster members be running. Because I have three members, one of the members should stop.</p>	<p>List information about the default scaling policies:</p> <p>Default scaling policies</p> <p>At least two cluster members are active</p> <p>Another cluster member starts when the average CPU, process memory u</p> <p>A cluster member stops when the average CPU, process memory, and hea</p>

Table 22. Demo changing a default scaling policy (continued). Mention the default scaling policies and demo changing a scaling policy.

Scene	Audio	Onscreen Action
14	I go to the scaling controller server.xml file and add a scaling definition that sets minimum equal to 1 and maximum equal to 2 for the default scaling policy.  Save the changes.	In the editor open on the server.xml file of the collective controller, add:  <pre>&lt;scalingDefinitions&gt;   &lt;defaultScalingPolicy enabled="true" min="1" max="2"/&gt; &lt;/scalingDefinitions&gt;</pre> Then, save the file changes.
15	The Explore tool shows that the scaling controller stopped one of the dynamic cluster members because of my change to the default scaling policy.  I have configured an auto-scalable cluster with JVM elasticity.	In the Explore tool, the number of stopped servers changes from 0 to 1. The status of myMember3 goes from running, to stopping, to stopped.

Table 23. Conclusion. Show where to find more information about auto scaling with JVM elasticity.

Scene	Audio	Onscreen Action
16	For more information about Liberty auto scaling and changing the default scaling policies, see WASdev.net and the WebSphere Application Server Liberty documentation on IBM Knowledge Center.	Show information on documentation:  <b>WASdev</b> <a href="http://developer.ibm.com/wasdev">http://developer.ibm.com/wasdev</a>  <b>WebSphere Application Server Liberty documentation on IBM Knowledge Center</b> <a href="http://www-01.ibm.com/support/knowledgecenter/">http://www-01.ibm.com/support/knowledgecenter/</a>

For more information, see “Configuring auto-scalable clusters for JVM elasticity” on page 1505.

## Video: Configuring an auto-scalable cluster for Liberty elasticity

8.5.5.7

The following transcript is for the “Configuring an auto-scalable cluster for Liberty elasticity” video, which demonstrates how to configure a collective to support Liberty server elasticity. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content shown in the video.

### Configuring an auto-scalable cluster for Liberty elasticity

Table 24. Title page. Show title and then animation that illustrates autonomic provisioning and then starting and stopping of servers based on resource use.

Scene	Audio	Onscreen Action
1	This video shows how to configure an auto-scalable cluster for Liberty elasticity.	Show title <i>Configuring an auto-scalable cluster for Liberty elasticity</i> .

Table 24. Title page (continued). Show title and then animation that illustrates autonomic provisioning and then starting and stopping of servers based on resource use.

Scene	Audio	Onscreen Action
2	<p>With Liberty elasticity, you have autonomic starting and stopping of cluster members based on scaling policies and resource use, just like with JVM elasticity.</p> <p>But you also have autonomic provisioning of new cluster members to other hosts.</p> <p>Even if a host doesn't have Liberty installed, Liberty elasticity can autonomously install on that host what's called a <i>stack</i> of Liberty software--the Liberty runtime, an IBM JRE, and a Liberty server with your applications--and then autonomously start and stop those installed Liberty servers and their applications. This gives you greater capacity to handle spikes in resource demand.</p> <p>What you see here is a scaling controller provisioning a stack group of Liberty software to hosts registered with the controller when resource use goes up, and then stopping or starting the provisioned cluster member servers and their applications in response to resource demands. You determine what Liberty software needs to be in a stack group based on what Liberty software is available on a registered host.</p>	<p>Show heading <i>Liberty elasticity auto scaling</i>.</p> <p>Show information <i>Autonomic starting and stopping of cluster members based on scaling policies and resource use (JVM elasticity)</i>. Show animation of a scaling controller starting and stopping Liberty server cluster members on a registered host computer. When an arrow representing resource use points upward, show scaling member servers on the registered host going from stopped to running. Then, when the arrow representing resource use points downward, show scaling member servers on the registered host going from running to stopped.</p> <p>Show information + <i>Autonomic provisioning of new cluster members to other hosts</i>. Show animation of a scaling controller provisioning new scaling members to two registered hosts and then starting and stopping those member servers based on the position of an arrow representing resource use.</p> <p>Show information <i>What's in a stack group?</i>. Show animation of a stack of Liberty software moving to two registered hosts. The registered host without an IBM JRE that supports Liberty servers in JAVA_HOME path receives:</p> <ul style="list-style-type: none"> <li>• Liberty runtime (wlp)</li> <li>• IBM JRE (wlp.jre)</li> <li>• Liberty server package (wlp.usr)</li> </ul> <p>The registered host with an IBM JRE that supports Liberty servers in JAVA_HOME path receives:</p> <ul style="list-style-type: none"> <li>• Liberty runtime (wlp)</li> <li>• Liberty server package (wlp.usr)</li> </ul>

Table 25. Demo configuring a scaling controller. Show configuring a scaling controller.

Scene	Audio	Onscreen Action
3	I begin by creating a server. At the wlp/bin directory of my Liberty installation, I run the server <b>create</b> command and name the server myController.	<p>Show heading <i>1 Configure a scaling controller</i>.</p> <p>Show a command window open at wlp/bin, and run a command that creates a server:</p> <pre>server create myController</pre> <p>Then show the message Server myController created.</p>
4	To make this server a collective controller, I run the collective <b>create</b> command. The command, by default, writes output to a console screen. You can specify the --createConfigFile option to write the output to a file instead.	In the command window open at wlp/bin, run a command that makes the server a collective controller:
5	I copy the output and paste it into the server.xml file of myController.	Show the generated controller configuration. Then, show marking and copying the configuration in the command window. And finally, show opening an editor on the wlp/usr/servers/myController/server.xml file and pasting the configuration into the file above the </server> tag.

Table 25. Demo configuring a scaling controller (continued). Show configuring a scaling controller.

Scene	Audio	Onscreen Action
6	<p>I specify adminUser and adminPassword for the controller administrative user name and password.</p> <p>I add host="*" to the httpEndpoint element. This is optional.</p> <p>To make myController a scaling controller, I add the scalingController-1.0 feature to a featureManager element.</p> <p>I also add the adminCenter-1.0 feature so I can view my collective in Admin Center. And finally, add a scaling policy. I begin with a scaling policy that is disabled and has a minimum and maximum of one server.</p>	<p>In the editor, show the following changes to the controller server.xml file:</p> <ol style="list-style-type: none"> <li>1. Add an administrative user name and password.  <code>&lt;quickStartSecurity userName="adminUser" userPassword="adminPassword"/&gt;</code>                      Show information <i>Add an administrative user name and password.</i></li> <li>2. Add host="*" to the httpEndpoint element.</li> <li>3. Add features to make myController a scaling controller and to enable administration of myController in Admin Center to a featureManager element.  <code>&lt;feature&gt;scalingController-1.0&lt;/feature&gt;</code>  <code>&lt;feature&gt;adminCenter-1.0&lt;/feature&gt;</code>                      Show information <i>The scalingController-1.0 feature is required for a scaling controller and then The adminCenter-1.0 feature is optional for a scaling controller but needed for this example to use Admin Center.</i></li> <li>4. Add a scaling policy that is disabled and has a minimum and maximum of one server.  <code>&lt;scalingDefinitions&gt;</code>  <code>  &lt;defaultScalingPolicy enabled="false" min="1" max="1"/&gt;</code>  <code>&lt;/scalingDefinitions&gt;</code>                      Show information <i>Add a scaling policy. Start with the scaling policy disabled.</i></li> <li>5. Save the file.</li> </ol>
7	<p>To start myController, run the server <b>start</b> command at a wlp/bin command line.</p>	<p>At an SSH service command line, enter commands that move to the wlp/bin directory and then start the controller.</p> <pre>cd /cygdrive/c/wlp/bin ./server start myController</pre> <p>Show information <i>On Windows computers, using an SSH service to start servers enables a controller to connect to member servers with SSH. The command runs and messages in the command window show myController started.</i></p>

Table 26. Demo going to the Servers page of the Admin Center Explore tool. Show opening a browser on Admin Center, logging in, and displaying the Servers page of the Explore tool.

Scene	Audio	Onscreen Action
8	<p>To view myController in Admin Center, open a browser on the <code>https://controller_host_name:controller_port_number/adminCenter/</code> URL.</p> <p>If your browser prompts you to confirm that the connection is trusted, specify an exception or otherwise enable the connection to Admin Center. Go to the Explore tool Servers page.</p>	<p>Show heading <i>Optional: View servers in Admin Center.</i></p> <p>In a web browser:</p> <ol style="list-style-type: none"> <li>1. Open the browser on the <code>https://controller_host_name:9443/adminCenter/adminCenter/</code> URL.</li> <li>2. Select to trust the connection.</li> <li>3. On the Admin Center login page, enter adminUser for the user name and adminPassword for the password. In the editor, highlight the user name and password in the scaling controller server.xml file at the same time to show needed login values.</li> <li>4. On the Toolbox page, select .</li> <li>5. In the Explore tool, select the Servers panel. The Explore tool shows one running server, myController.</li> </ol>

Table 27. Demo configuring a scaling member. Show creating a server, joining it as a member server to the controller, and then configuring it to be a scaling member.

Scene	Audio	Onscreen Action
9	I now make a scaling member. At a wlp/bin command prompt, I run the server <b>create</b> command and name the server myMember.	Show heading 2 <i>Configure a scaling member</i> .  Show command window open at wlp/bin, and run: server create myMember  Then show the message Server myMember created.
10	To join this server to the collective, I run the collective <b>join</b> command. You can get the --host, --port, --user and --password values from the controller server.xml file. For --keystorePassword, set a value to use for the member keystore password. The --hostName parameter is optional.	In command window open at wlp/bin, run: collective join myMember --host=controller_host_name --hostName=host_name --port=9443 --use  After a message asking whether to accept the certificate chain displays, enter y.
11	I now copy the output and paste it into the myMember server.xml. You can specify the --createConfigFile option to write the output to a file instead.	Show marking and copying the generated configuration in the command window. Then, show opening an editor on the wlp/usr/servers/myMember/server.xml file and pasting the configuration into the file above the </server> tag.

Table 27. Demo configuring a scaling member (continued). Show creating a server, joining it as a member server to the controller, and then configuring it to be a scaling member.

Scene	Audio	Onscreen Action
12	<p>In the member server.xml file, I set the RPC user and password, which are the user name and password that I enter to log on to this Windows computer. The user must have administrative privileges on the computer.</p> <p>In this example, the controller and member are on the same host, so I need to change the port numbers. If your member server is on a different host from the controller, ensure the ports are unique on that host.</p> <p>Add the scalingMember-1.0 feature to make the member server a scaling member.</p> <p>Add a hostSingleton element and set its port to a number that is unique on the host. The host singleton port is used by all Liberty servers on the same host to elect a leader. The job of the leader is to report aggregated scaling metrics for all servers on the host. If the leader stops running, another leader is elected.</p>	<p>In the editor, show the following changes to the member server.xml file:</p> <ol style="list-style-type: none"> <li>1. Set the RPC user and password, which is the user name and password that you enter to log on to the computer. The user must have administrative privileges on the computer.  <pre>&lt;hostAuthInfo rpcUser="admin_user_id"               rpcUserPassword="admin_user_password" /&gt;</pre> </li> <li>2. Change the port numbers from 9080 to 9081 and 9443 to 9444 so that the member ports are different from the controller ports and from other ports used on the computer.  <pre>&lt;httpEndpoint id="defaultHttpEndpoint"               httpPort="9081"               httpsPort="9444" /&gt;</pre> </li> <li>3. Make myMember a scaling member by adding scalingMember-1.0 to a featureManager element.  <pre>&lt;feature&gt;scalingMember-1.0&lt;/feature&gt;</pre> <p>Show information <i>The scalingMember-1.0 feature is required for a scaling member. You can add both clusterMember-1.0 and scalingMember-1.0 or add only scalingMember-1.0. You don't need clusterMember-1.0 because the scalingMember-1.0 feature enables the clusterMember-1.0 feature.</i></p> </li> <li>4. Add a hostSingleton element and set its port to 5164 or any other port that is unique on the computer.  <pre>&lt;hostSingleton name="ScalingMemberSingletonService" port="5164" /&gt;</pre> <p>Show information <i>A scaling member server.xml file must define a hostSingleton element with a port. All scaling members on the same host must use the same port. You can specify any port number, but the port number must be unique on the host computer. This example uses port number 5164.</i></p> </li> <li>5. Save the file.</li> </ol> <p>On the Admin Center Explore tool Servers page, myMember is shown as stopped.</p>
13	<p>Start myMember.</p>	<p>At an SSH service command line on the wlp/bin directory, start the scaling member.</p> <pre>./server start myMember</pre> <p>The command runs and the messages showing myMember started display in the command window. On the Admin Center Explore tool Servers page, myMember is shown as started.</p>

Table 28. Demo verifying that JVM elasticity auto scaling is working. Show enabling the scaling policy, with the auto scaling icon displaying on the Servers page of the Admin Center Explore tool, and then disabling the scaling policy.

Scene	Audio	Onscreen Action
14	I want to test the auto scaling. In the controller server.xml file, I enable the scaling policy and save the file.	<p>Show heading <i>Optional: Test the scaling configuration.</i></p> <p>In the editor open on the controller server.xml file, enable auto scaling. Change:  <code>&lt;defaultScalingPolicy enabled="false" min="1" max="1"/&gt;</code>                      to:  <code>&lt;defaultScalingPolicy enabled="true" min="1" max="1"/&gt;</code></p> <p>On the Admin Center Explore tool Servers page, the auto scaling icon  displays on the myMember card, indicating that the scaling policy is enabled. Show information <i>When scaling policies are enabled, scaling members have an auto scaling icon in Admin Center.</i></p>
15	At this time, the configuration has JVM elasticity. The scaling controller can start and stop scaling members based on scaling policies and resource use.	<p>To verify that JVM elasticity auto scaling is working, change the min value to 0 in the editor:  <code>&lt;defaultScalingPolicy enabled="true" min="0" max="1"/&gt;</code></p> <p>Show information <i>Setting the minimum to 0 (zero) stops the scaling member.</i> On the Admin Center Explore tool Servers page, myMember status changes from started to stopped, indicating that JVM elasticity auto scaling is working.</p>
16		<p>In the editor open on the controller server.xml file, change the min value back to 1:  <code>&lt;defaultScalingPolicy enabled="true" min="1" max="1"/&gt;</code></p> <p>Show information <i>Setting the minimum to 1 (one) restarts the scaling member.</i> On the Admin Center Explore tool Servers page, myMember status changes from stopped to started, indicating that JVM elasticity auto scaling is working.</p>
17	Because I haven't yet set up the configuration for Liberty elasticity, I disable the scaling policy.	<p>In the editor open on the controller server.xml file, disable auto scaling.  <code>&lt;defaultScalingPolicy enabled="false" min="1" max="1"/&gt;</code></p> <p>Show information <i>Testing confirms that auto scaling is working. For this example, temporarily disable scaling policies until the stack group and its installables and packages are defined.</i> On the Admin Center Explore tool Servers page, the auto scaling icon  is no longer shown on the myMember card, indicating that scaling policies are disabled.</p>

Table 29. Demo adding a stack group cluster name to the member server.xml file. Show assigning the member to myStackGroup.cluster1. By default, cluster members are in defaultCluster.

Scene	Audio	Onscreen Action
18	<p>In the member server.xml file, I add a statement that puts the member in a cluster named myStackGroup.cluster1. I am going to make the myStackGroup directory and put installables and packages for Liberty elasticity auto scaling into it. You can use the default stack group name, defaultStackGroup. cluster1 is the name of the server package that I'm going to make.</p> <p>If your collective has other dynamic cluster members, add the same statement to the other member server.xml files so they belong to the same cluster.</p>	<p>Show heading 3 <i>Add the scaling member to a cluster named stack_group_name.provisionable_cluster_name.</i></p> <p>In the editor open on the member server.xml file, add a statement that puts the member in a cluster named myStackGroup.cluster1:  <code>&lt;clusterMember name="myStackGroup.cluster1"/&gt;</code></p> <p>Show information <i>myStackGroup is the name of the stack group directory that will hold installables and packages for Liberty elasticity auto scaling and cluster1 is the name of the server package that the scaling controller will provision to registered hosts.</i> On the Admin Center Explore tool Servers page, the name of the cluster for myMember changes from defaultCluster to myStackGroup.cluster1.</p>

Table 30. Demo registering a target host. Show running the registerHost command to register a target host with the collective controller.

Scene	Audio	Onscreen Action
19	<p>I want Liberty elasticity auto scaling to install cluster1 on a different host.</p> <p>I run the collective <b>registerHost</b> command and specify a Linux machine for the target host. You can run additional <b>registerHost</b> commands and register more than one target host.</p>	<p>Show heading 4 <i>Register a host, to which the scaling controller will provision servers based on scaling policies.</i></p> <p>Show a command window open at wlp/bin, and then run a command to register the target host:  <code>collective registerHost target_host_name --host=controller_host_name --port=9443 --user=</code></p> <p>After a message asking whether you want to accept the certificate chain displays, enter y. Then show a message confirming the host registered successfully.</p>
20		<p>In Admin Center, select , the Dashboard icon, to return to the Explore tool Dashboard, select the Hosts panel, show that the registered host has been added, and then return to the Servers page.</p>
21	<p>If the registered host has no Liberty software, which is the case here, then the stack group needs to contain a Liberty runtime, IBM JRE, and a Liberty server package with applications.</p>	<p>Show the file system of the registered host.</p> <p>Show information <i>For this example, the registered host does not have Liberty or an IBM JRE that supports Liberty installed. Liberty elasticity auto scaling will need to provision to the registered host:</i></p> <ul style="list-style-type: none"> <li>• Liberty runtime installable (wlp)</li> <li>• JRE installable (wlp.jre)</li> <li>• Server package (wlp.usr)</li> </ul>

Table 31. Demo creating the stackGroups/myStackGroup directories. Show creating the wlp/usr/shared/stackGroups/myStackGroup directory with its installables and packages subdirectories.

Scene	Audio	Onscreen Action
22	<p>I'm now going to create the myStackGroup directory. This directory name is the same as what's in the cluster name.</p> <p>I copy the defaultStackGroup directory, and rename it.I'll be putting Liberty software that I want the scaling controller to install on the registered host in the installables and packages subdirectories.</p>	<p>Show heading <i>Optional: Create your own stack group subdirectories if you don't want to use the default stack group.</i></p> <p>Show a file system browser and move to the wlp/usr/shared/stackGroups directory. Copy the defaultStackGroup directory, paste it into the stackGroups directory, and rename the pasted directory myStackGroup. Then show the installables and packages subdirectories.</p>

Table 32. Demo creating the Liberty runtime installable and adding it to the stackGroups/myStackGroup/installables directory. Show running a **package** command to create wlp.855.zip and then adding the file to the wlp/usr/shared/stackGroups/myStackGroup/installables directory.

Scene	Audio	Onscreen Action
23		<p>Show heading <i>5 Create a Liberty runtime installable named the wlp.name.zip naming convention.</i></p> <p>Show a file system browser and move to the wlp_installable directory. Show that the directory is empty.</p>
24	<p>To create a Liberty runtime archive, I run the server <b>package</b> command with the --include=wlp option. This creates an archive that contains the wlp directory, but does not contain the usr directory. The archive name, wlp.855.zip, follows the naming convention.</p>	<p>Show a command window open at wlp/bin, and then run a <b>package</b> command to create a Liberty runtime installable named wlp.855.zip to go in the wlp_installable empty directory:</p> <pre>server package --include=wlp --archive=c:\wlp_installable\wlp.855.zip</pre> <p>The command runs and the messages show c:\wlp_installable\wlp.855.zip packaging completed.</p>
25	<p>Copy the archive to the stack group installables directory.</p>	<p>In the file system browser, copy wlp.855.zip and paste it into the wlp/usr/shared/stackGroups/myStackGroup/installables directory.</p>

Table 33. Demo creating the JRE installable and adding it to the `stackGroups/myStackGroup/installables` directory. Show compressing the contents of the `java` directory of a Liberty JRE installation to create `jre.17.zip` and then adding the file to the `wlp/usr/shared/stackGroups/myStackGroup/installables` directory.

Scene	Audio	Onscreen Action
26	<p>To create an IBM JRE that supports Liberty servers, zip up the contents of the <code>java</code> directory of the JRE used for Liberty.</p> <p>Move the archive to the stack group <code>installables</code> directory.</p>	<p>Show heading 6 <i>Create a JRE installable named with the <code>jre.name.zip</code> naming convention if the registered host doesn't have or use an IBM JRE that supports Liberty servers.</i></p> <p>Show a file system browser and move to the <code>java</code> directory of a Liberty JRE installation. Show compressing the contents of the <code>java</code> directory to create <code>jre.17.zip</code>. Then copy the file and paste it into the <code>wlp/usr/shared/stackGroups/myStackGroup/installables</code> directory.</p> <p>Show information: <i>The JRE installable must be appropriate for the operating system of the registered hosts</i></p>

Table 34. Demo creating the `cluster1` server package and adding to the `myStackGroup/packages` directory. Show running the `create` command to create a server named `cluster1`, pasting an application into the `dropins` directory of `cluster1`, running a `package` command to create `cluster1.zip`, and then adding the file to the `wlp/usr/shared/stackGroups/myStackGroup/packages` directory.

Scene	Audio	Onscreen Action
27	<p>To create the <code>cluster1</code> server package, create a server named <code>cluster1</code>.</p>	<p>Show heading 7 <i>Create a server package, which the scaling controller will provision to the registered host based on scaling policies. This example packages a server named <code>cluster1</code> that has an application in its <code>dropins</code> directory..</i></p> <p>Show a command window open at <code>wlp/bin</code>, and run:  <code>server create cluster1</code></p> <p>Then show the message <code>Server cluster1 created.</code></p>
28	<p>Add one or more applications to it.</p>	<p>In a file system browser, paste an application into <code>wlp/usr/servers/cluster1/dropins</code> to add an application to the server.</p>
29	<p>And run the <b>server package cluster1</b> command with the <code>--include=usr</code> option. This creates a server package that contains the <code>usr</code> directory, but does not contain all the Liberty runtime files.</p>	<p>In the command window at <code>wlp/bin</code>, run:  <code>server package cluster1 --include=usr</code></p> <p>Then show the message confirming package creation and its location.</p> <p>Show information: <i>For Windows registered hosts, create a <code>server.env</code> file that sets <code>JAVA_HOME</code> to the JRE location on the registered hosts. Place the <code>server.env</code> in the same directory as the <code>server.xml</code> in the server package ZIP. Example <code>server.env</code> file contents: <code>JAVA_HOME=C:\wlp\jre\jre.17.zip\jre</code></i></p>
30	<p>Copy the zip file to the stack group <code>packages</code> directory.</p>	<p>In the file system browser, copy <code>wlp/usr/servers/cluster1/cluster1.zip</code> and paste it into the <code>wlp/usr/shared/stackGroups/myStackGroup/packages</code> directory.</p>

Table 35. Demo setting a user name and password for the stack manager in the scaling controller server.xml file. Show adding a stackManager element with the administrative user name and password to the scaling controller server.xml file.

Scene	Audio	Onscreen Action
31	In the controller server.xml file, add a statement that sets the user name and password for the stack manager.	Show heading 8 Add a stackManager element to the scaling controller configuration.  In the editor open on the scaling controller server.xml file, add a statement that sets the administrative user name and password for the stack manager: <code>&lt;stackManager controllerUser="adminUser" controllerUserPassword="adminPassword" /&gt;</code>  Then, save the file.

Table 36. Demo changing the scaling policy to force the scaling controller to provision a new server on the registered host. Show changing the scaling policy in the scaling controller server.xml file to enable auto scaling and require a minimum of two servers. Then show a server added to the Admin Center Explore tool Servers page.

Scene	Audio	Onscreen Action
32	I'm now ready to test the Liberty elasticity auto scaling. I can force the scaling controller to provision the Liberty software to the registered host by increasing the min and max values and enabling the scaling policy.  After I save the changes, I wait for Admin Center to display the provisioned member server. As you can see, the scaling controller installed a cluster1 member on the registered host then started the member and its application.	Show heading 9 Set scaling policy min and max values that force the scaling controller to provision a new server, and enable scaling policies.  In the editor open on the scaling controller server.xml file, increase the min and max values from 1 to 2 and enable auto scaling by changing enabled from false to true: <code>&lt;scalingDefinitions&gt;   &lt;defaultScalingPolicy enabled="true" min="2" max="2"/&gt; &lt;/scalingDefinitions&gt;</code>  Then, save the changes.  Show information Provisioning installables and a server package to a registered host can take several minutes. The Admin Center Explore tool Servers page shows a cluster1 server provisioned on the registered host. Its status changes from stopped to started.
33	Liberty elasticity auto scaling is working so I set the min and max values to what I want for the auto scaling. The provisioned member will start and stop based on scaling policies and resource use.	In the editor open on the scaling controller server.xml file, decrease the min value from 2 to 1: <code>&lt;scalingDefinitions&gt;   &lt;defaultScalingPolicy enabled="true" min="1" max="2"/&gt; &lt;/scalingDefinitions&gt;</code>  Then, save the changes.  Show information This example sets min=1 and max=2 for the minimum and maximum number of member servers available for auto scaling. You can set a higher maximum, such as max=4, to enable additional cluster1 member servers to be provisioned on the registered host. The scaling controller can start provisioned member servers when resource use increases and stop the member servers when resource use decreases. The Admin Center Explore tool Servers page shows the provisioned cluster1 server status change from started to stopped, or from stopped to started, indicating that Liberty elasticity auto scaling is working.

*Table 37. Show new directories and files on the registered host. Show that the registered host now has the wlp, wlp.jre, and wlp.usr directories for the Liberty runtime and JRE installables and cluster1 server package on the registered host.*

Scene	Audio	Onscreen Action
34		Show heading <i>Registered host before auto scaling</i> with a screen capture of a file system browser on the registered host, which has no wlp directories. Show heading <i>Registered host after auto scaling</i> with a screen capture of the file system browser on the registered host with the wlp, wlp.jre, and wlp.usr directories.
35	The registered host now has the wlp, wlp.jre, and wlp.usr directories for the Liberty runtime and JRE installables and cluster1 server package.	Show heading <i>Registered host after auto scaling</i> . Show a screen capture of the file system browser on the registered host with the wlp, wlp.jre, and wlp.usr directories for the Liberty runtime and JRE installables and cluster1 server package highlighted. Show information <i>Liberty runtime installable, IBM JRE installable, and cluster1 server package</i> .

*Table 38. Conclusion. Show where to find more information about auto scaling with Liberty elasticity.*

Scene	Audio	Onscreen Action
36	For more information about auto scaling in Liberty, see WASdev.net and the Liberty documentation on IBM Knowledge Center.	Show the following text:  For more information about Liberty auto scaling, see:  <b>WASdev</b> <a href="http://developer.ibm.com/wasdev">http://developer.ibm.com/wasdev</a>  <b>WebSphere Application Server Liberty documentation on IBM Knowledge Center</b> <a href="http://www.ibm.com/support/knowledgecenter/">http://www.ibm.com/support/knowledgecenter/</a>

For more information, see “Configuring provisionable clusters for Liberty elasticity” on page 1506.

## Video: DevOps with WebSphere Liberty Server

8.5.5.5

The following transcript is for the “DevOps with WebSphere Liberty Server” video, which demonstrates how to develop, build and deploy an application with Liberty server DevOps and some open source tools. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content that is shown in the video.

### Demo - DevOps with WebSphere Liberty Server

*Table 39. Title page. Show title and then a basic overview of building, updating, testing, and deploying an application.*

Scene	Audio	Onscreen Action
1	This demo will show you how to provide the capability for building and deploying your application with WebSphere Liberty Server and a set of common open source tools.	Show title <i>Demo - DevOps with WebSphere Liberty Server</i> .
2	You will use Git for source control, use WebSphere Application Server Developer Tools to develop your application, and use Maven for build.	Show image of <i>1. Develop and Build Application</i> that uses the following options <ul style="list-style-type: none"> <li>• Git</li> <li>• WebSphere Developer Tools (WDT)</li> <li>• Maven</li> </ul>

Table 39. Title page (continued). Show title and then a basic overview of building, updating, testing, and deploying an application.

Scene	Audio	Onscreen Action
3	You will also make changes to your web application running in Liberty and push changes from Eclipse IDE to production environment.	Show image of 2. <i>Update Application</i> that uses WDT.
4	You will use Apache Maven together with the WebSphere Liberty Maven plug-in to run integration test to verify your changes.	Show image of 3. <i>Test Application</i> with the Liberty Maven plug-in.
5	You will also use Jenkins for continuous integration.	Show image of 4. <i>Continuous Integration</i> that uses Jenkins.
6	You will use Chef to push a new build to the production environment.  Liberty will be the Java Platform, Enterprise Edition run time for all the above DevOps scenarios. We will use an Airline application - AcmeAir as a sample in this demo. It will demonstrate a controllable and highly repeatable DevOps practice.	Show image of 5. <i>Continuous Deploy</i> that uses Chef.

Table 40. Demo of Developing and Building an Application

Scene	Audio	Onscreen Action
7	<p>Now lets start the first scenario: develop and build your application.</p> <p>Open Eclipse, which has WDT already preinstalled.</p> <ol style="list-style-type: none"> <li>1. We will set the workspace preference for use with Maven.</li> <li>2. Then we will clone a Git repository containing the AcmeAir application, specify the Git repository URI.</li> <li>3. Then we will import the set of Maven based AcmeAir projects: There are 5 Maven-based projects in this repository.</li> <li>4. Now we can run the Maven build to build the projects and create application artifacts. Make sure the build is successful when it finishes.</li> <li>5. Now we can create a Liberty server to run our application from Eclipse: So specify the Liberty install directory.</li> <li>6. And also name the Liberty server.</li> <li>7. Then we can open the server.xml to config the server to run our AcmeAir application. <ul style="list-style-type: none"> <li>• First we will specify the &lt;httpEndpoint&gt; endpoint.</li> <li>• And we will also add the database configuration, which refers to a Derby database for application data.</li> </ul> </li> <li>8. Start the WebSphere Liberty server and the AcmeAir application.</li> <li>9. Now login to the application and experience it.</li> <li>10. You can select your destination and the city from which you depart. Check those available airline tickets and book it.</li> </ol>	<p>Show title <i>Step 1 Develop and Build Application</i>.</p> <p>Demo showing the following steps to develop and build an application that uses WDT.</p> <p>Open Eclipse, which has WDT preinstalled.</p> <ol style="list-style-type: none"> <li>1. Set the workspace preferences for use with Maven. Click the <b>Set all Maven values</b> button.</li> <li>2. We will clone a Git repository containing the AcmeAir application by specify the Git repository URI.</li> <li>3. Import the set of Maven-based AcmeAir projects: The acmeair repository contains 5 Maven-based projects.</li> <li>4. Now run Maven to build the projects and create the application artifacts. Make sure that the build is successful when it finishes.</li> <li>5. Now we can create a WebSphere Liberty server to run the application from Eclipse: Specify the Liberty install directory.</li> <li>6. Name the server AcmeAirDemo and add the acmeair-webapp application into it.</li> <li>7. Open the server configuration server.xml file to configure the Liberty server for service. <ul style="list-style-type: none"> <li>• Replace the &lt;httpEndpoint&gt; element and add further configuration.</li> <li>• Add the database configuration, which refers to a Derby database for application data.</li> </ul> </li> <li>8. Start the WebSphere Liberty server and AcmeAir application.</li> <li>9. Click the <b>application URL</b> to verify that the application is active. Initialize the application by loading the flight data set.</li> <li>10. Now AcmeAir is ready for use. <ul style="list-style-type: none"> <li>• Logins to the application and click the <b>Flights</b> action and type in New York under <b>Leave From</b> and Paris under <b>Arrive At</b>.</li> <li>• Click the <b>Find Flights</b> or <b>Browse Flights</b> button.</li> <li>• Pick any outbound flight and select it by clicking it.</li> <li>• Pick any return flight and select it by clicking it.</li> <li>• Click the <b>Book Select Flights</b> button.</li> </ul> </li> </ol>

Table 41. Demo updating application

Scene	Audio	Onscreen Action
8	In scenario 2 we will make a quick change to our application and show how to do a continuous delivery with that. To simplify the scenario we will just make a very small change to our indexed page. To replace some highlighted content with ""Welcome to Acme Air"". Now after you save these changes, you can refresh to see that the change is in effect.	Show title <i>Step 2 Update Application</i>  Demo showing the Index page that is being updated in the application.

Table 42. Demo testing the application

Scene	Audio	Onscreen Action
9	<p>Next we will use Maven and the Liberty Maven plug-in for integration tests.</p> <ol style="list-style-type: none"> <li>1. The AcmeAir application has a acmeair-itests project that contains integration tests.</li> <li>2. To enable of the integration tests we will need to edit our pom.xml file. There are a few changes we need to make here, but the most important one is that we will enable and config the Liberty Maven plug-in to start the Liberty server before our integration tests and to stop the server after the tests are done.</li> <li>3. We will create a run Configuration for AcmeAir integration tests. <ul style="list-style-type: none"> <li>• Click the <b>Run</b> button to run the integration tests. It will take a few minutes to allow the tests to complete. So its build successfully.</li> <li>• Examine the console output to see the Liberty Maven plug-in starting the server before the tests run and to stop it after the test.</li> </ul> </li> <li>4. You can view the test report and make sure there is no error in the result.</li> <li>5. Next we will push the pom.xml change to Git so that the itests can be run in a Jenkins build.</li> </ol>	<p>Demo testing the application, that uses the following steps</p> <ol style="list-style-type: none"> <li>1. The AcmeAir application has a acmeair-itests project that contains integration tests.</li> <li>2. Enable activation of integration tests by editing the acmeair-itests/pom.xml file.</li> <li>3. Enable the Build Helper Maven plug-in to find an available network port.</li> <li>4. Enable and configure the Liberty Maven plug-in to start the Liberty server before integration tests are executed and stop the server after the tests are done.</li> <li>5. Enable and configure the Maven Failsafe plug-in to execute the integration tests. The tests exercise the REST API of the application.</li> <li>6. Create a run Configuration for AcmeAir integration tests. <ul style="list-style-type: none"> <li>• Click the <b>Run</b> button to run the integration tests. The tests should complete successfully.</li> <li>• Examine the console output to see the Liberty Maven plug-in starting the server before the tests run.</li> <li>• Examine the console output to see the Liberty Maven plug-in stopping the server after the tests.</li> </ul> </li> <li>7. View the test reports under target/failsafe-reports/ directory.</li> <li>8. Push the pom.xml change to Git so the itests can be run in a Jenkins build.</li> </ol>

Table 43. Demo showing continuous integration with Jenkins

Scene	Audio	Onscreen Action
10	<ol style="list-style-type: none"> <li>1. In the next scenario we will use Jenkins to create and run a build job for the AcmeAir application. The job will check out the application code from Git, compile the application, execute the tests, and publish the build artifacts. With the configuration in Schedule, the job will poll the Git repository every two minutes and automatically start a build if any changes are detected. <ul style="list-style-type: none"> <li>• Specify the Liberty install directory.</li> <li>• We will also add a <b>post-build action</b> and choose <b>Archive the artifacts</b>.</li> <li>• After a minute or 2 the build should automatically start.</li> </ul> </li> <li>2. Once the build completes and is successful, examine the build job results. The <b>Test Result</b> should indicate there is no failure.</li> <li>3. Switch back to Eclipse and commit the changes made on the Index page.</li> <li>4. Switch back to Jenkins and you will see within 2 minutes a new build should appear under the <b>Build History</b> table.</li> </ol>	<p>Show title <i>Step 4 Continuous Integration</i></p> <p>Demo showing continuous integration with Jenkins using the following steps:</p> <ol style="list-style-type: none"> <li>1. We will use Jenkins to create and run a build job for the AcmeAir application. The job will check out the application code from Git, compile the application, execute the tests, and publish the build artifacts. With the configuration in Schedule, the job will poll the Git repository every two minutes and automatically start a build if any changes are detected. <ul style="list-style-type: none"> <li>• We will click the <b>Add post-build actions</b> button and choose <b>Archive the artifacts</b>.</li> <li>• After a minute or 2 a build should automatically start.</li> </ul> </li> <li>2. Once the build completes and is successful, examine the build job results. The acmeair-webapp-1.0-SNAPSHOT.war file should appear under <b>Build Artifacts</b> and <b>Test Result</b> should indicate no failures.</li> <li>3. Switch back to Eclipse and commit the changes that are made on the Index page.</li> <li>4. Switch to Firefox and go to <code>http://server:9080/jenkins/job/AcmeAir tests/</code> address. Within 2 minutes a new build should appear under the <b>Build History</b> table. <ul style="list-style-type: none"> <li>• Click the new build and verify that the right commit message appears under <b>Changes</b>.</li> </ul> </li> </ol>

Table 44. Demo showing continuous deployment with Chef

Scene	Audio	Onscreen Action
11	<p>1. In the last scenario we will do a continuous deployment with Chef.</p> <ul style="list-style-type: none"> <li>• Open a terminal window.</li> <li>• Create an empty cookbook</li> <li>• Edit the metadata file of the cookbook</li> <li>• Edit the recipe file</li> <li>• Upload the AcmeAir cookbook to the Chef server</li> </ul> <p>2. Also register the template node with the Chef server.</p> <p>3. You can config the template node configuration on the Chef server.</p> <p>4. Then you can populate the Chef node. This will cause the <b>chef-client</b> command to run on the template node. The AcmeAir application should be fully deployed and running on the template node. To verify that, switch to Firefox and open the template application server to check the results.</p> <p>5. Then we will create a new Jenkins build job to invoke <b>chef-client</b> on the template node to update it, only after all the integration tests pass.</p> <ul style="list-style-type: none"> <li>• On the Jenkins console, edit the AcmeAir tests job.</li> <li>• Under <b>Post-build Actions</b> click on <b>Add post-build action</b> and choose <b>Build other projects</b>.</li> <li>• Under <b>Projects to build</b> type in AcmeAir-Chef.</li> <li>• Verify that the AcmeAir tests job triggers the AcmeAir-Chef job by requesting a AcmeAir tests build.</li> </ul> <p>We just demonstrate DevOps practice with Liberty and common open source tools. You can now try the full End to End DevOps scenarios all together repeatedly. While in this demo we choose Chef, WDT, Maven, and Jenkins, these technologies can easily be interchangeable with other DevOps tools like uDeploy®, Puppet, etc,, Thanks for watching.</p>	<p>Show title <i>Step 5 Continuous Deploy</i></p> <p>Demo showing continuous deployment with Chef that uses the following steps:</p> <ol style="list-style-type: none"> <li>1. Create a cookbook to deploy AcmeAir <ul style="list-style-type: none"> <li>• Open a terminal window.</li> <li>• Create an empty cookbook</li> <li>• Edit the metadata file of the cookbook</li> <li>• Edit the default.rb recipe file</li> <li>• Upload the AcmeAir cookbook to the Chef server</li> </ul> </li> <li>2. Bootstrap the Chef node and register the template node with the Chef server.</li> <li>3. Configure the template node configuration on the Chef server.</li> <li>4. Populate the Chef node. Execute the <b>knife ssh name:template sudo chef-client</b> command. This will cause the <b>chef-client</b> command to run on the template node. <b>chef-client</b> will execute a set of cookbooks on the node. The AcmeAir application should be fully deployed and running on the template node. To verify, switch to Firefox and open the http://template:9081/acmeair/ address.</li> <li>5. Populate the Chef node automatically with Jenkins. We will create a new Jenkins build job that will invoke <b>chef-client</b> on the template node to update it, only after all the integration tests pass. <ul style="list-style-type: none"> <li>• On the Jenkins console, edit the AcmeAir tests job.</li> <li>• Under <b>Post-build Actions</b> click <b>Add post-build action</b> and choose <b>Build other projects</b>.</li> <li>• Under <b>Projects to build</b> type in AcmeAir-Chef.</li> <li>• Verify that the AcmeAir tests job triggers the AcmeAir-Chef job by requesting a new AcmeAir tests build.</li> </ul> </li> </ol>

## Video: Enabling IHS for Liberty Dynamic Routing

8.5.5.5

The following transcript is for the “Enabling IHS for Liberty Dynamic Routing” video, which demonstrates how to install IBM HTTP Server (IHS), install the Web Server Plug-in for WebSphere Application Server, and apply the interim fix for Dynamic Routing. You must enable IHS first before

setting up the Dynamic Routing feature or using auto scaling with Liberty collectives. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content shown in the video.

## Enabling IHS for Liberty Dynamic Routing

*Table 45. Demo installing IBM Installation Manager.* Show installing IBM Installation Manager.

Scene	Audio	Onscreen Action
1	This video shows how to install and enable IHS for Dynamic Routing using the IBM Installation Manager.	Show title Enabling IHS for Liberty Dynamic Routing.
2	Download and install the latest version of the IBM Installation Manager. You can use the Installation Manager to access online product repositories to install the Web Server Plug-in for WebSphere Application Server and the needed interim fix for the Dynamic Routing feature.	Direct user to the IBM Installation Manager and begin installing the latest version.
3	Once I select the latest version to install I click <b>Download package</b> from the installation menu. I then selected the platform I wanted to download and the appropriate fix for my machine. In this demo I will be installing the IBM Installation Manager Kit for Windows 64. You will be prompted for your IBM user ID and password before you can proceed with the download.	Show the user how to install the appropriate IBM Installation Kit from the IBM support site.
4	Select your download options. In this demo I will download the IBM Installation Manager using my browser (HTTPS). Click <b>Continue</b> . Download the provided zip file to your machine. You can locate this zip file in your downloads folder. Right click on the zip file in your downloads folder and click <b>Extract Files...</b> You must then select the location where you want to install the contents of the zip file.	Show the user how to download the IBM Installation Manager using a browser. Show the user how to download the zip file to their machine and extract the content to a new designated location.
5	When all of the files have been extracted successfully, open the folder containing the files and click <b>install.exe</b> The IBM Installation Manager will open and begin downloading. Accept the terms in the license agreements, and click <b>Next</b> . Verify that the install package is downloading in the appropriate directory, and click <b>Next</b> . Click <b>Install</b> . The IBM Installation Manager will now be installed.	Show the user how to run the install from the <code>install.exe</code> file. The user must accept the terms and license agreements to proceed with the install. Once they click Install the IBM Installation Manager will begin installing.
6	You will see a confirmation window when the install has been completed successfully. On this Window click <b>Restart Installation Manager</b> . Once the restart is complete, you can begin using the IBM Installation Manager.	Show the user the confirmation window that confirms the IBM Installation Manager was successfully downloaded. Show the user how to restart the IBM Installation Manager prior to using.

Table 46. Demo Set preferences for repository locations. Show how to set preferences for repository locations.

Scene	Audio	Onscreen Action
7	Start the Installation Manager and click <b>File</b> . Then click <b>Preferences</b> . Then click <b>Add Repository</b> to add the repository URL to the product. You can access repository URLs for the product via the Passport Advantage Online. Follow the same steps to add the repository URL needed to install the Web Server Plug-in for WebSphere Application Server	<p>Show user how to start the Installation Manager and add repository URLs. Users can gain access to repository URLs via the Passport Advantage Online. For more information on how to download repository URLs from Passport Advantage, go to the IBM Support Portal.</p> <p><b>IBM Support Portal-</b>  <a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038625">http://www-01.ibm.com/support/docview.wss?uid=swg27038625</a></p> <p>Show the user how to add the following repository URL for installing the Web Server Plug-in.</p> <p><b>Web Server Plug-in for WebSphere Application Server</b> <a href="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.PLGILAN.v85">http://www.ibm.com/software/repositorymanager/com.ibm.websphere.PLGILAN.v85</a></p>

Table 47. Demo installing IBM HTTP Server. Show installing IBM HTTP Server.

Scene	Audio	Onscreen Action
8	Start the Installation Manager and click <b>Install</b> . In the <b>Install Packages</b> window select the appropriate version of <b>IHS</b> . Click <b>Next</b> . Accept the terms in the license agreements, and click <b>Next</b> .	Show users how to start the Installation Manger and locate IHS in the <b>Install Packages</b> window. Show them how to begin the installation and accept terms in the license agreements.
9	On the install packages window, specify the installation directory where you would like to install IHS. Click <b>Next</b> . On the next window IHS will already be selected for you. Click <b>Next</b> .	<p>Show the user an example of how to specify the installation directory. Note the following restrictions:</p> <ul style="list-style-type: none"> <li>• Deleting the default target location and leaving an installation-directory field empty prevents you from continuing. Do not use symbolic links as the destination directory.</li> <li>• Symbolic links are not supported.</li> <li>• Be careful on using spaces in the name of the installation directory. Some operating systems allow spaces in the specification of the installation directory. Other operating systems do not allow spaces.</li> <li>• Do not use a semicolon in the directory name. IBM HTTP Server cannot install properly if the target directory includes a semicolon.</li> </ul>
10	On the Configuration for IHS panel, specify your web server configuration. Specify a port number on which IHS will communicate. The default port is 80. Choose whether to use a Windows service to run IHS. Click <b>Next</b> .	Show users how to specify the web server configuration and specify the port number for IHS.
11	Review the summary information, and click <b>Install</b> . You will see a confirmation window if the installation was successful. Click <b>Finish</b> . <b>Note:</b> You don't have to start IHS until you're ready to use the Dynamic Routing or Auto Scaling features.	Show the user an example of summary information and the final step of installation. If the installation is successful, a message appears indicating the installation completed successfully.

Table 48. Demo installing Web Server Plug-in for WebSphere Application Server. Show installing Web Server Plug-in for WebSphere Application Server using IBM Installation Manager.

Scene	Audio	Onscreen Action
12	You already added the repository URL needed to install the Web Server Plug-in. Start the Installation Manager and click <b>Install</b> . In the <b>Install Packages</b> window select the appropriate version of the <b>Web Server Plug-in for WebSphere Application Server</b> . Click <b>Next</b> . Accept the terms in the license agreements, and click <b>Next</b> .	Show users how to start the Installation Manger and locate IHS in the <b>Install Packages</b> window. Show them how to begin the installation and accept terms in the license agreements.
13	On the install packages window, specify the installation directory where you would like to install the Web Server Plug-in. Click <b>Next</b> . On the next window the Web Server Plug-in will already be selected for you. Click <b>Next</b> .	Show the user an example of how to specify the installation directory. Note the following restrictions: <ul style="list-style-type: none"> <li>• Deleting the default target location and leaving an installation-directory field empty prevents you from continuing. Do not use symbolic links as the destination directory.</li> <li>• Symbolic links are not supported.</li> <li>• Be careful on using spaces in the name of the installation directory. Some operating systems allow spaces in the specification of the installation directory. Other operating systems do not allow spaces.</li> <li>• Do not use a semicolon in the directory name. IBM HTTP Server cannot install properly if the target directory includes a semicolon.</li> </ul>
14	Review the summary information, and click <b>Install</b> . You will see a confirmation window if the installation was successful. Click <b>Finish</b> .	Show the user an example of summary information and the final step of installation. If the installation is successful, a message appears indicating the installation completed successfully.

Table 49. Demo how to update the IBM HTTP Server. Updating the IBM HTTP Server

Scene	Audio	Onscreen Action
15	Start the Installation Manager. Click <b>Update</b> . Select the package group to update. Click <b>Next</b> . Select the version you want to update under <b>IHS</b> .	Show users how to locate and apply the interim fix for Dynamic Routing using the Installation Manager and IHS.
16	Review the summary information, and click <b>Update</b> . You will see a confirmation window if the installation was successful. Click <b>Finish</b> .	Show the user an example of summary information and the final step of installation. Done successfully a message will appear indicating a successful installation.

Table 50. Conclusion. Show where to find more information about Dynamic Routing and auto scaling.

Scene	Audio	Onscreen Action
17	For information on configuring clustered Liberty collectives for use with Dynamic Routing or Auto Scaling, see WASdev and the WebSphere Application Server Liberty documentation on IBM Knowledge Center.	Show information on documentation: <p><b>WASdev</b>  <a href="https://developer.ibm.com/wasdev/">https://developer.ibm.com/wasdev/</a></p> <p><b>WebSphere Application Server Liberty documentation on IBM Knowledge Center</b>  <a href="http://www-01.ibm.com/support/knowledgecenter/">http://www-01.ibm.com/support/knowledgecenter/</a></p>

For more information, see “Setting up dynamic routing for Liberty collectives” on page 1493.

# Video: Getting started with the Server Configuration Tool for WebSphere Liberty

8.5.5.8

The following transcript is for the “Getting started with the Server Configuration Tool for WebSphere Liberty” video, which demonstrates how to enable and use the Liberty Admin Center Server Config tool. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content that is shown in the video.

## Getting started with the Server Configuration Tool for WebSphere Liberty

Table 51. Title page. Show title and describe the video contents.

Scene	Audio	Onscreen Action
1	This video demonstrates the new web-based WebSphere Liberty server configuration tool. This tool makes it possible to view and edit server configuration files from a web browser.	Show title “Getting started with the Server Configuration Tool for WebSphere Liberty”.

Table 52. Demo enabling the Server Config tool. Show how to enable the Server Config tool.

Scene	Audio	Onscreen Action
2	To enable it, simply add the adminCenter-1.0 feature, keyStore, and quickStartSecurity elements to your server.xml file.  Optionally, if you are planning to use the tool to make changes to the server configuration, add the remote file access element.	Show a server.xml file with elements needed to enable the Server Config tool and enable editing: <pre>&lt;server&gt;   &lt;featureManager&gt;     &lt;feature&gt;adminCenter-1.0&lt;/feature&gt;   &lt;/featureManager&gt;    &lt;keyStore password="samplePassword"/&gt;    &lt;quickStartSecurity userName="sampleUser" userPassword="samplePassword"/&gt;    &lt;remoteFileAccess&gt;     &lt;writeDir&gt;\${server.config.dir}&lt;/writeDir&gt;   &lt;/remoteFileAccess&gt; &lt;/server&gt;</pre>
3	After saving these changes, a URL will appear in the server console.  Open this URL with your favorite web browser.	Show a console message and selecting the URL to the tool: Starting server configuration update Web application available: http://localhost:9080/ibm/adminCenter/serverConfig-1.0/ The server is ready to run a smarter planet.
4	Log in with the quickStartSecurity credentials.	Show entering sampleUser and samplePassword on the login page of Admin Center.

Table 53. Demo using the Server Config tool. Show how to view and edit server configuration files with the Server Config tool.

Scene	Audio	Onscreen Action
5	The file selection screen shows all of the configuration files available on the server. If nested include files are found, these will be hierarchically shown in the form of a tree.	Show the Configuration Files page of the Server Config tool.  Show expanding the primary list of files under server.xml.

Table 53. Demo using the Server Config tool (continued). Show how to view and edit server configuration files with the Server Config tool.

Scene	Audio	Onscreen Action
6	<p>To edit a file simply click on its name. This brings up the main editing screen.</p> <p>The tree shows all of the configuration elements in the document. Clicking on a tree node displays all of its associated values.</p> <p>Values can be edited by typing on the text fields or using the selection buttons. If a mistake is made, automatic validation provides instant feedback.</p>	<p>Show selecting <code>server.xml</code> to display the contents of the <code>server.xml</code> file in <b>Design</b> mode.</p> <p>Show selecting the <b>HTTP Endpoint</b> element to display its values.</p> <p>Show selecting a new value, the display of a warning message, and selecting <b>x</b> to delete the value change.</p>
7	Adding new elements is very easy. Simply click on the <b>Add child</b> button and select the element to be added.	Show selecting <b>Add child</b> , an element, and <b>Add</b> .
8	Removing elements is just as easy. Simply click on the <b>Remove</b> button and provide confirmation.	Show selecting <b>Remove</b> and then <b>Remove</b> to confirm the removal.
9	The order of the elements can be changed at any time using drag-and-drop gestures.	Show dragging an element to a different location in the tree.
10	The source of the document can be accessed by clicking the <b>Source</b> tab.	Show selecting the <b>Source</b> tab to display the <code>server.xml</code> source.
11	Syntax highlight, hover information, and content assist features are available.	Show hovering a cursor over an element value in the source to display information about the value.
12	After changes are complete, click on the <b>Save</b> button to persist them on the server.	Show selecting <b>Save</b> .

Table 54. Conclusion. State that the video is now ending.

Scene	Audio	Onscreen Action
13	This concludes the WebSphere Liberty server configuration tool video. Thanks for watching!	Show Copyright 2015 IBM Corporation. Voice over provided by Colleen Anderson. and then Thanks for watching!

For more information, see “Editing server configuration files in Admin Center” on page 1748.

## Video: Google OpenID Connect for applications on WebSphere Liberty

8.5.5.5

The following transcript is for the “Google OpenID Connect for applications on WebSphere Liberty” video, which demonstrates how to set up an OpenID Connect web single-sign-on on WebSphere Application Server Liberty with a Google OpenID Connect provider. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content that is shown in the video.

 Google OpenID Connect for applications on WebSphere Liberty

Table 55. Title page. Show title and then a basic Google OpenID Connect scenario.

Scene	Audio	Onscreen Action
1	This video will show you how to set up OpenID Connect web single-sign-on on WebSphere Application Server Liberty with a Google OpenID connect provider.	Show title <i>OpenID Connect Quick Setup with Google</i> .
2	Here you can see an “OpenID Connect” flow from an end user to an application on the Liberty server and the Google OpenID provider. When a user first attempts to access a Google OpenID Connect-protected application on a Liberty server, the user is redirected to the Google OpenID Provider. By using the Google account, the user is authenticated to access the protected web application on the Liberty server. In this video, we call a Liberty server, the “Relying party” or RP, and call “Google OpenID Connect provider” the OP.	Show a basic Google OpenID Connect scenario, that includes a Relying Party (RP), Google OpenID Connect provider (OP), and an End-User.

Table 56. Demo registering Liberty in Google

Scene	Audio	Onscreen Action
3	<p>To set up the Liberty RP with Google OP, first, we will register the Liberty server as an OpenID Connect client in the Google OP.</p> <p>To do so, we will</p> <ul style="list-style-type: none"> <li>• Log in to the Google developers console and create a project</li> <li>• Then in the project, we will create a “Client ID” for the Liberty server</li> <li>• Write down the Client ID and Client Secret for when we set up Liberty</li> </ul> <p>Let's try these steps now.</p>	<p>Show title <i>Register Liberty in Google</i>.</p> <ol style="list-style-type: none"> <li>1. On Google developer's console, create a project <a href="https://console.developers.google.com">https://console.developers.google.com</a>.</li> <li>2. In the project, create a Client ID from the <b>Credential</b> menu.</li> <li>3. Write down the following information for the Liberty setup <ul style="list-style-type: none"> <li>• Client ID</li> <li>• Client Secret</li> </ul> </li> </ol> <p>For more information, please refer to this page <a href="https://developers.google.com/accounts/docs/OpenIDConnect">https://developers.google.com/accounts/docs/OpenIDConnect</a>.</p>
4	In the Google Developers Console, create a new Project.	<p>In the Google Developers Console, we show a demo creating a new project.</p> <ul style="list-style-type: none"> <li>• Project name- WebSphereLibertyOpenIDConnect</li> <li>• Project ID- astute-tome-859</li> </ul>
5	In the project that you just created, go to <b>APIs &amp; auth</b> , then <b>Credentials</b> , and <b>Create new Client ID</b> . First, you will have to configure a consent screen.	Show the Google Developers Console screen where the <b>Create new Client ID</b> is selected.

Table 56. Demo registering Liberty in Google (continued)

Scene	Audio	Onscreen Action
6	The consent screen is shown to users when they authenticate with the Google OpenID provider. Configure your consent screen as needed and continue creating your Client ID. For the application type, select <b>Web application</b> . Then, enter a redirect URI for the Liberty server. (pointing to <code>https://rp-example.rtp.raleigh.ibm.com:7778/oidcclient/redirect/oidcRP</code> on the screen) This redirect URI comes from the configuration for your Liberty server, which we will cover later. If you don't know the redirect URI for your server, you can leave the default value and update it later.	Show the Google Developers Console screen where the <b>Web Application</b> is selected. <ul style="list-style-type: none"> <li>Authorized JavaScript Origins is set to <code>https://www.example.com</code></li> <li>Authorized Redirect URIs is set to <code>https://www.example.com/oauth2callback</code></li> </ul>
7	After the Client ID is created, you can see the Client ID and Client Secret. Make note of these values, because they are needed in the next step, configuring the Liberty server.	Show the Google Developers Console screen where the Client ID and Client Secret values can be seen.

Table 57. Demo configuring WebSphere Liberty

Scene	Audio	Onscreen Action
8	To set up Liberty to work with a Google OP, you will need to: <ul style="list-style-type: none"> <li>Install Version 8.5.5.5 or later of Liberty</li> <li>Install the OpenID Client feature</li> <li>Create a Liberty server</li> <li>Edit the <code>server.xml</code> configuration file with Google information</li> <li>Install the application that will use the Google account for authentication</li> <li>And finally, import the Google certificate into the keystore for SSL communication</li> </ul>	Show the WebSphere Liberty setup overview. <ol style="list-style-type: none"> <li>Install WebSphere Liberty 8.5.5.5 or latest beta &gt; <b>java -jar wlp-developers-runtime-8.5.5.5.jar</b></li> <li>Install OpenID Client feature (No download necessary) &gt; <b>bin/featureManager install openidConnectClient-1.0 --when-file-exists=ignore</b></li> <li>Create a Liberty server &gt; <b>server create GoogleRP</b></li> <li>Edit the <code>server.xml</code> with more configurations (Sample downloadable) <ul style="list-style-type: none"> <li>Required features</li> <li>SSL keystore</li> <li>OpenID Client</li> <li>Application</li> </ul> </li> <li>Install application that will use Google account for authentication &gt; Copy application ear/war file under app directory.</li> <li>Import Google certificate into keystore for SSL communication.</li> </ol>
9	First, we will install Version 8.5.5.5 of Liberty.  Then, we will install the OpenID Client feature, and create a server with the name GoogleRP.  You can find the <code>server.xml</code> configuration file under the <code>wlp\usr\servers\GoogleRP\</code> directory.	Demo with command prompt that is being used to update <code>server.xml</code> file.
10	Here is the default <code>server.xml</code> file. Now, we will compare it to a <code>server.xml</code> file that has a Google configuration.	Show a default <code>server.xml</code> file.

Table 57. Demo configuring WebSphere Liberty (continued)

Scene	Audio	Onscreen Action
11	<p>You can see that the necessary features are added. In the OpenID Connect Client configuration, the Client ID and Client Secret that we obtained from Google are added. You can obtain the other values by going to Google OP's discovery endpoint. (<a href="https://accounts.google.com/.well-known/openid-configuration">https://accounts/google.com/.well-known/openid-configuration</a> is shown on the video). Then we add an SSL configuration and end-point configuration with the host name, HTTP port, and HTTPS port.</p> <p>The configuration file also includes configuration for applications that rely on Google to perform authentication.</p> <p>That's all the configuration we need for Liberty.</p> <p>The Liberty RP uses this pattern <code>https://&lt;hostname&gt;:&lt;sslport&gt;/oidcclient/redirect/&lt;openidConnectClient id&gt;</code> to generate its own redirect URL. For example, the server that we configured has the following URI, <code>https://rp-example.rtp.raleigh.ibm.com:7778/oidcclient/redirect/oidcRP</code>. This is the URI that we entered earlier in the Google console.</p>	<p>Show a <code>server.xml</code> file that contains the Client ID and Client Secret that were obtained from Google. Also an SSL configuration and end-point configuration with the host name, HTTP port, and HTTPS port. The <code>server.xml</code> file also includes configuration for applications that rely on Google to perform authentication.</p>
12	<p>Next, we will install our application in the app directory.</p> <p>We will start and stop the Liberty server to get the keystore in the server resources and make sure that the Liberty server keystore has a Google certificate for SSL communication.</p> <p><b>Note:</b> We are not going to show cert steps in this video and include instruction in reference page</p> <p>Then we will start the Liberty server again.</p>	<p>Show title <i>How to import Google certificate here.</i></p>

Table 58. Demo testing the setup

Scene	Audio	Onscreen Action
13	<p>Now we will test our configuration to see if it works.</p> <ul style="list-style-type: none"> <li>In a browser, we will go to the application URL.</li> <li>When prompted, we will enter our Google account information.</li> <li>We will see the application redirecting to Google to perform authentication.</li> <li>After the user is authenticated, the RP will show an application page to the user.</li> <li>Let's try that now.</li> </ul>	<p>Demo testing the setup.</p> <ol style="list-style-type: none"> <li>Start the WebSphere Liberty server &gt; <b>server start oidcRP</b></li> <li>In a browser, point to the application login page on the Liberty Server &gt; <code>http://rp-example.rtp.raleigh.ibm.com:7777/testpage</code></li> <li>When prompted, enter the Google user ID and password &gt; <code>xxx.yyy@gmail.com / mypassword</code></li> <li>Application relies on Google to perform authentication</li> <li>User is successfully authenticated</li> </ol>

Table 58. Demo testing the setup (continued)

Scene	Audio	Onscreen Action
14	In the browser, we will type in the URL of the application that is running on the Liberty server. Notice that we are prompted by the Google OP server because the Liberty relying party is delegating the authentication to the OP. We will enter the credentials for the Google account. After accepting the consent screen, we are successfully logged in to the application on the RP using the OP account.	Demo with a browser login that shows a successful login into the application on the RP using the OP account.

Table 59. Conclusion. Show where to find more information about OpenID Connect that uses Google.

Scene	Audio	Onscreen Action
15	For more information, visit these online resources.	<p>Show information on documentation:</p> <p><b>WebSphere Liberty download page</b>  <a href="https://developer.ibm.com/wasdev/downloads/liberty-profile-using-non-eclipse-environments/">https://developer.ibm.com/wasdev/downloads/liberty-profile-using-non-eclipse-environments/</a></p> <p><b>OpenID Connect feature installation</b>            Server: <a href="https://developer.ibm.com/wasdev/downloads/#asset/features-com.ibm.websphere.appserver.openidConnectServer-1.0">https://developer.ibm.com/wasdev/downloads/#asset/features-com.ibm.websphere.appserver.openidConnectServer-1.0</a>            Client: <a href="https://developer.ibm.com/wasdev/downloads/#asset/features-com.ibm.websphere.appserver.openidConnectClient-1.0">https://developer.ibm.com/wasdev/downloads/#asset/features-com.ibm.websphere.appserver.openidConnectClient-1.0</a></p> <p><b>IBM Knowledge Center - OpenID Connect main page</b>  <a href="http://www-01.ibm.com/support/knowledgecenter/api/content/nl/en-us/SSAW57_8.5.5/com.ibm.websphere.wlp.nd.multipatform.doc/ae/rwlp_using_oidc.html">http://www-01.ibm.com/support/knowledgecenter/api/content/nl/en-us/SSAW57_8.5.5/com.ibm.websphere.wlp.nd.multipatform.doc/ae/rwlp_using_oidc.html</a></p> <p><b>All OpenID Connect attributes are discussed here</b>  <a href="http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.wlp.doc/ae/twlp_config_oidc_rp.html?cp=SSEQTP_8.5.5%2F1-3-11-0-4-2-9-2">http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.wlp.doc/ae/twlp_config_oidc_rp.html?cp=SSEQTP_8.5.5%2F1-3-11-0-4-2-9-2</a></p> <p><b>IBM DeveloperWorks OpenID Connect article</b>  <a href="http://www.ibm.com/developerworks/websphere/library/techarticles/1502_odonnell/1502_odonnell.html">http://www.ibm.com/developerworks/websphere/library/techarticles/1502_odonnell/1502_odonnell.html</a></p> <p><b>WebSphere Liberty OpenID Connect setup video on YouTube</b>  <a href="http://youtu.be/fuajCS5bG4c">http://youtu.be/fuajCS5bG4c</a></p> <p><b>Google setup "OpenID Connect (OAuth 2.0 for Login)"</b> <a href="https://developers.google.com/accounts/docs/OpenIDConnect">https://developers.google.com/accounts/docs/OpenIDConnect</a></p>

For more information about OpenID Connect, see [8.5.5.5](#) Using OpenID Connect.

## Video: Health management for Liberty collectives

8.5.5.7

The following transcript is for the “Health management for Liberty collectives” video, which demonstrates the benefits of using health management in your Liberty environment. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content shown in the video.

### Health management for Liberty collectives

*Table 60. Introduction and overview. Show title and introduce health management.*

Scene	Audio	Onscreen Action
1	Do your applications use too much memory, have memory leaks or slow response time? Health management in Liberty can help find and mitigate problems in your applications as they occur.	Show title <i>Health management for Liberty collectives</i> .
2	Health management in a Liberty collective can prevent the disruption of service by detecting common problems and generating diagnostic actions based on configured health policies.	Show words:  Prevent disruption of service  Use policies to detect app health concerns: <ul style="list-style-type: none"> <li>• Excessive memory usage</li> <li>• Memory leaks</li> <li>• Excessive request timeout</li> <li>• Excessive average response time</li> </ul>
3	You can target health policies at individual servers, all servers in a cluster, or all servers on a host.	Show diagram of server clusters with hosts and highlight each section.
4	To diagnose and manage errors, health policies can capture heap or thread dumps, restart servers, and force servers to enter maintenance mode.	Show words:  Health policies can: <ul style="list-style-type: none"> <li>• Capture heap and thread dumps</li> <li>• Restart servers</li> <li>• Force servers into maintenance mode</li> </ul>

*Table 61. Feature and JVM configuration for health management.. Show the process for configuring health management.*

Scene	Audio	Onscreen Action
5	You can add support for health management to your Liberty collectives through the healthManager-1.0 and healthAnalyzer-1.0 features. After you set up a collective, add the healthManager-1.0 feature to a collective controller. If you want to monitor excessive memory usage or memory leaks, add the healthAnalyzer-1.0 feature to a collective member server.	Show code for adding healthManager-1.0 to a collective controller server.xml file and adding healthAnalyzer-1.0 to a collective member server.xml file.

Table 62. Health policy configuration for health management.. Show an example of a health policy configuration for health management.

Scene	Audio	Onscreen Action
6	<p>To configure a health policy, add a healthPolicy element to the collective controller server.xml file. You can configure multiple policies by adding additional healthPolicy elements.</p> <p>Each health policy has one or more targets, one condition, and one or more actions.</p> <p>The target can be a cluster, a host, or a server. This healthPolicy element targets a single server.</p> <p>The condition that triggers corrective action is excessive average response time of at least 10 seconds. When this condition exists, the affected server is put into maintenance mode. If you specify multiple actions, the actions run in the order that they are specified in the policy.</p>	<p>Show a controller server.xml file with the example healthPolicy element highlighted.</p> <pre data-bbox="846 352 1450 485">&lt;healthPolicy id="myPolicy"&gt;   &lt;server hostName="Host" wlpUsrDirectory="ibm/liberty/wlp" serv   &lt;excessiveResponseTime responseTime="10s"/&gt;   &lt;action action="enterMaintenanceMode"/&gt; &lt;/healthPolicy&gt;</pre>
7	<p>Let's take a look at this policy in action.</p> <p>The healthManager-1.0 feature is enabled in a collective controller that is configured for dynamic routing and auto-scaling.</p>	<p>Show a controller server.xml file with the example healthPolicy element highlighted.</p> <pre data-bbox="846 877 1450 1266">&lt;featureManager&gt;   &lt;feature&gt;jsp-2.2&lt;/feature&gt;   &lt;feature&gt;collectiveController-1.0&lt;/feature&gt;   &lt;feature&gt;dynamicRouting-1.0&lt;/feature&gt;   &lt;feature&gt;scalingController-1.0&lt;/feature&gt;   &lt;feature&gt;healthManager-1.0&lt;/feature&gt; &lt;/featureManager&gt;  ...  &lt;healthPolicy id="myPolicy"&gt;   &lt;server hostName="Host" wlpUsrDirectory="ibm/liberty/wlp" serv   &lt;excessiveResponseTime responseTime="10s"/&gt;   &lt;action action="enterMaintenanceMode"/&gt; &lt;/healthPolicy&gt;</pre>
8	<p>The Intelligent Management IBM HTTP Server plug-in detects average response times of over 10 seconds for Server 1. In accordance with the health policy, the controller forces Server 1 into maintenance mode, and IBM HTTP Server stops routing new requests to that server.</p> <p>As Server 1 goes into maintenance mode, the scaling controller simultaneously detects that fewer than two servers are running and starts Server 3. IBM HTTP Server begins routing requests to that server.</p>	<p>Show animation of a server being put into maintenance mode, another server starting, and traffic being routed to the newly started server.</p>

Table 63. Conclusion. Show where to find more information about health management.

Scene	Audio	Onscreen Action
9	For more information about health management and Liberty collectives, see the Knowledge Center documentation or WASdev.net.	Show information on documentation:  <b>IBM Knowledge Center</b> <a href="http://www-01.ibm.com/support/knowledgecenter/">http://www-01.ibm.com/support/knowledgecenter/</a>  <b>WASdev.net</b> <a href="http://developer.ibm.com/wasdev">http://developer.ibm.com/wasdev</a>

For more information, see “Configuring health management for Liberty” on page 1519.

## Video: Installing Liberty from a ZIP file

8.5.5.6

The following transcript is for the “Installing Liberty from a ZIP file” video, which describes how you can quickly install Liberty from a ZIP archive file, start the server and add applications, and upgrade to a supported installation. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content that is shown in the video.

### Installing Liberty from a ZIP file

Table 64. Installing and upgrading Liberty. Show how you can quickly install IBM WebSphere Application Server Liberty from a ZIP archive file, start the server and add applications, and upgrade to a supported installation.

Scene	Audio	Onscreen Action
1	Installing WebSphere Application Server Liberty can be as easy as extracting a ZIP file!	Show words, “Installing Liberty from a ZIP file”
2	To start, download one of the Liberty runtime ZIP files from IBM Fix Central or WASdev.net. You can choose from several prepackaged archives according to your needs, from just the Liberty kernel, which has a download size of less than 15 megabytes, to the Java Platform, Enterprise Edition 7 full platform or Web Profile, which you can optionally download with IBM Java 8.	Show the ZIP files on IBM Fix Central and WASdev.net.
3	After you download a ZIP file, just extract it to a local directory to install Liberty.	Show extracting the wlp-webProfile7-8.5.5.6 ZIP archive file to the C:\wlp-webProfile7-8.5.5.6 directory.

Table 64. Installing and upgrading Liberty (continued). Show how you can quickly install IBM WebSphere Application Server Liberty from a ZIP archive file, start the server and add applications, and upgrade to a supported installation.

Scene	Audio	Onscreen Action
4	This example shows the Java EE 7 Web Profile ZIP, which comes preconfigured with Liberty features that support the Java EE 7 Web Profile specification.	Show running the <b>productInfo featureInfo</b> command on the command line. A list of installed features is displayed.
5	You can install additional features and other content using the <b>installUtility</b> command. The <b>find</b> option displays a list of installable content.	Show running the <b>installUtility find</b> command on the command line. A list of installable features, addons, samples, and other content is displayed.
	Start the Liberty server with the <b>server start</b> command.	Show running the <b>server start</b> command on the command line. The default server, <code>defaultServer</code> , starts.
	<p>You can add an application at any time by placing the application WAR file in the <code>dropins</code> directory - no restart required!</p> <p>The Liberty server automatically starts the application when you add it to the directory.</p> <p>Standard server output and errors are captured in the <code>console.log</code> file; for example, this application outputs the URL of the web application, which can then be pasted into the browser.</p>	<p>Show copying the <code>planningpoker-1.0-SNAPSHOT.war</code> sample application into the <code>wlp\usr\servers\defaultServer\dropins</code> directory.</p> <p>Show opening the <code>console.log</code> file in the <code>wlp\usr\servers\defaultServer\logs</code> directory to copy the URL of the web application and pasting the URL into the browser. The web application loads successfully.</p>
	Installing from the ZIP files enables no-charge, unsupported, unlimited use of Liberty in development environments and unsupported limited use in small-scale test and production environments.	Show running the <b>productInfo version</b> command on the command line. The product name, version, and edition is displayed. Because the installation is an unsupported version, the edition is <code>BASE_ILAN</code> .

Table 64. *Installing and upgrading Liberty (continued)*. Show how you can quickly install IBM WebSphere Application Server Liberty from a ZIP archive file, start the server and add applications, and upgrade to a supported installation.

Scene	Audio	Onscreen Action
	<p>For access to guaranteed service levels and IBM support, you can later upgrade to a supported edition from your existing installation. After you purchase WebSphere Application Server, just download and run the self-extracting license JAR file from Passport Advantage®.</p> <p>Note that if you are already a WebSphere Application Server customer - for example, if you are running Network Deployment traditional - you do not need to purchase anything extra; the Liberty entitlement is included.</p>	<p>Show copying the <code>wlp-nd-license.jar</code> file into the <code>C:\wlp-webProfile7-8.5.5.6</code> directory.</p> <p>Show running the <code>java -jar wlp-nd-license.jar</code> command on the command line to run the self-extracting JAR file. The command updates the license.</p> <p>Show running the <code>productInfo version</code> command, which now displays the ND edition.</p>
	<p>For more information about installing and upgrading Liberty, see the Knowledge Center documentation or WASdev.net.</p>	<p>Show words, "For more information about installing and upgrading Liberty, see:"</p> <ul style="list-style-type: none"> <li>• IBM Knowledge Center</li> <li>• WASdev.net</li> </ul>

For more information, see "Installing Liberty by extracting a ZIP archive file" on page 1381.

## Video: Introduction to creating a collective

The following transcript is for the "Introduction to creating a Liberty collective" video, which demonstrates how to create a collective of one controller and one member. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content shown in the video.

### Introduction to creating a Liberty collective

Table 65. *Demo creating a Liberty collective*. Show commands and `server.xml` changes.

Scene	Audio	Onscreen Action
1	<p>Hi, I'm Mike Thompson, a developer with WebSphere Liberty. I'm going to take you today through a brief introduction of Liberty's new administrative domain known as the collective.</p>	<p>Show the developer talking on camera.</p>

Table 65. Demo creating a Liberty collective (continued). Show commands and server.xml changes.

Scene	Audio	Onscreen Action
2	Starting with a Liberty Network Deployment install, we're going to create a simple collective. This can be done in about eight steps. The first step is creating a server to be the administrative server. I'm going to call that myController.	Show command window open at wlp/bin, run server create myController, and then show message Server myController created.
3	Once the server myController is created, we then need to establish the collective configuration necessary for the server to act as a controller. As part of that configuration, we're going to specify a keystore password. The keystore password is not predefined. We do not ship predefined user names or passwords. So, using the keystore password demoPassword will establish the configuration for a collective controller.	Show command window open at wlp/bin, and then run the command: collective create myController --keystorePassword=demoPassword

Table 65. Demo creating a Liberty collective (continued). Show commands and server.xml changes.

Scene	Audio	Onscreen Action
4	This takes about three seconds and essentially establishes some SSL certificates. We need to copy the configuration printed to the screen and update the server configuration file.	Show messages generated by the command, with the following messages marked for copying: <pre>&lt;featureManager&gt;   &lt;feature&gt;collectiveController-1.0&lt;/feature&gt; &lt;/featureManager&gt;  &lt;!-- Define the host name for use by the collective.   If the host name needs to be changed, the server should be   removed from the collective and re-joined or re-replicated. --&gt; &lt;variable name="defaultHostName" value="myhost.ibm.com" /&gt;  &lt;!-- TODO: Set the security configuration for Administrative access --&gt; &lt;quickStartSecurity userName="" userPassword="" /&gt;  &lt;!-- clientAuthenticationSupported set to enable bidirectional trust --&gt; &lt;ssl id="defaultSSLConfig"   keyStoreRef="defaultKeyStore"   trustStoreRef="defaultTrustStore"   clientAuthenticationSupported="true" /&gt;  &lt;!-- inbound (HTTPS) keystore --&gt; &lt;keyStore id="defaultKeyStore" password="{xor}OzoyMA8+LCwoMC07"   location="\${server.config.dir}/resources/security/key.jks" /&gt;  &lt;!-- inbound (HTTPS) truststore --&gt; &lt;keyStore id="defaultTrustStore" password="{xor}OzoyMA8+LCwoMC07"   location="\${server.config.dir}/resources/security/trust.jks" /&gt;  &lt;!-- server identity keystore --&gt; &lt;keyStore id="serverIdentity" password="{xor}OzoyMA8+LCwoMC07"   location="\${server.config.dir}/resources/collective/serverIdentity.jks" /&gt;  &lt;!-- collective trust keystore --&gt; &lt;keyStore id="collectiveTrust" password="{xor}OzoyMA8+LCwoMC07"   location="\${server.config.dir}/resources/collective/collectiveTrust.jks" /&gt;  &lt;!-- collective root signers keystore --&gt; &lt;keyStore id="collectiveRootKeys" password="{xor}OzoyMA8+LCwoMC07"   location="\${server.config.dir}/resources/collective/rootKeys.jks"/&gt;</pre>
5	We can do that using Notepad because this is very simple XML and we can essentially paste it right into the contents of the server.xml.	Show a Notepad editor open on the myController server.xml file, and then the copied messages pasted into the server.xml file before the ending tag, </server>.
6	In addition to pasting it in, we do need to specify an administrative name. So, I'm going to use admin, with adminpwd as the password.	In editor, set user name and password: <pre>&lt;quickStartSecurity userName="admin" userPassword="adminpwd" /&gt;</pre>
7	Once the server is configured, we can start it.	Show command window open at wlp/bin, run server start myController, and then show message: Starting server myController

Table 65. Demo creating a Liberty collective (continued). Show commands and server.xml changes.

Scene	Audio	Onscreen Action
8	<p>Now that the collective controller is running, I can create a server to join to the collective. I'm going to create a server called myMember and I'll join this server into the collective. This operation can be done using the collective <b>join</b> command. And, what needs to be specified is the host and port that the collective controller is listening on the HTTPS port, the administrative user name and password, and a keystore password. This password can be the same or different from the password used when we created the collective controller.</p>	<p>Show command window open at wlp/bin, run <code>server create myMember</code>, and show message            Server myMember created.</p> <p>Then run <code>collective join myMember --host=localhost --port=9443 --user=admin --password=adminpwd --keystorePassword=demoPassword</code>.</p>
9	<p>Because this is connecting over SSL to the collective controller, it will prompt us for SSL trust. The certificate presented here is from the collective controller, which we recognize. We will accept the certificate and what will happen in the background is that the collective controller will establish some SSL certificates that will be handed back and laid down in the file system for this particular member.</p>	<p>Show messages generated by the <b>collective join</b> command. The messages show that the Issuer DN is controllerRoot. After the message Do you want to accept the above certificate chain? (y/n), enter y to accept the certificate.</p>

Table 65. Demo creating a Liberty collective (continued). Show commands and server.xml changes.

Scene	Audio	Onscreen Action
10	<p>We copy the configuration, just like we did for the controller, and we update the member's configuration file.</p> <p><b>Important:</b> <span style="background-color: #0056b3; color: white; padding: 2px;">8.5.5.4</span> The generated configuration has a <code>hostAuthInfo</code> element that was added to the product after the video was made. Complete the <code>hostAuthInfo</code> element in either of two ways:</p> <ul style="list-style-type: none"> <li>Specify the operating system login user ID and password for an authorized user of the member host computer. For example, if you log in to the member computer using the user ID <code>user1</code> and password <code>user1pwd</code>, you can specify: <pre>&lt;hostAuthInfo rpcUser="user1" rpcUserPassword="user1pwd" /&gt;</pre> </li> <li>If the member host is registered with the collective controller, you can specify: <pre>&lt;hostAuthInfo useHostCredentials="true" /&gt;</pre> </li> </ul>	<p>Show messages generated about keystore and truststore references, with the following messages marked for copying:</p> <pre>&lt;featureManager&gt;   &lt;feature&gt;collectiveMember-1.0&lt;/feature&gt; &lt;/featureManager&gt;</pre> <pre>&lt;!-- Define the host name for use by the collective.   If the host name needs to be changed, the server should be   removed from the collective and re-joined or re-replicated. --&gt;</pre> <pre>&lt;variable name="defaultHostName" value="memberHostname" /&gt;</pre> <p><span style="background-color: #0056b3; color: white; padding: 2px;">8.5.5.4</span> <code>&lt;!-- Remote host authentication configuration --&gt;</code> <code>&lt;hostAuthInfo rpcUser="admin_user_id" rpcUserPassword="admin_user_password" /&gt;</code>  <code>&lt;!-- Connection to the collective controller --&gt;</code> <code>&lt;collectiveMember controllerHost="localhost" controllerPort="9443" /&gt;</code> <code>&lt;!-- clientAuthenticationSupported set to enable bidirectional trust --&gt;</code> <code>&lt;ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore" trustStoreRef="defaultTrustStore" clientAuthenticationSupported="true" /&gt;</code>  <code>&lt;!-- inbound (HTTPS) keystore --&gt;</code> <code>&lt;keyStore id="defaultKeyStore" password="yourPassword" location="{server.config.dir}/resources/security/key.jks" /&gt;</code> <code>&lt;!-- inbound (HTTPS) truststore --&gt;</code> <code>&lt;keyStore id="defaultTrustStore" password="yourPassword" location="{server.config.dir}/resources/security/trust.jks" /&gt;</code> <code>&lt;!-- server identity keystore --&gt;</code> <code>&lt;keyStore id="serverIdentity" password="yourPassword" location="{server.config.dir}/resources/collective/serverIdentity.jks" /&gt;</code> <code>&lt;!-- collective truststore --&gt;</code> <code>&lt;keyStore id="collectiveTrust" password="yourPassword" location="{server.config.dir}/resources/collective/collectiveTrust.jks" /&gt;</code></p>
11	<p>We can do that also using Notepad.</p>	<p>Show the command to open a Notepad editor, <code>notepad usr/servers/myMember/server.xml</code>, show a Notepad editor open on the <code>myMember</code> <code>server.xml</code> file, and then the copied messages pasted into the <code>server.xml</code> file before the ending tag, <code>&lt;/server&gt;</code>.</p>
12	<p>Once updated, the member server can be started and the member server will start publishing its information into the controller.</p> <p>And that's it. You now have a very basic collective. To add more members, you just repeat the join operation on any servers that you want to create. It's that easy. The members are added and the collective grows.</p>	<p>Show command window open at <code>wlp/bin</code>, run <code>server start myMember</code>, and then show messages:</p> <pre>Starting server myMember Server myMember started</pre>

For more information, see “Configuring a Liberty collective” on page 1136.

## Video: Java EE 7 in Liberty

8.5.5.6

The following transcript is for the “Java EE 7 in Liberty ” video, which describes Liberty support for the Java Platform, Enterprise Edition (Java EE) 7 specifications and highlights ways to enable your Liberty servers for Java EE 7. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content that is shown in the video.

 Java EE 7 in Liberty

Table 66. Title page and benefits of Java EE 7. Show title and then list the benefits of Java EE 7.

Scene	Audio	Onscreen Action
1	Liberty now complies with Java Platform, Enterprise Edition Version 7. This video tells you about Liberty support for Java EE 7 and shows how you can quickly configure your servers for it.	Show title <i>Java EE 7 in Liberty</i> and the Java Compatible Enterprise Edition logo. Also show <i>Java Platform, Enterprise Edition Version 7</i> instead of <i>Java EE 7</i> for a few seconds to give the full name for <i>Java EE 7</i> .
2	<p>With Java EE 7, you have an open framework that enables you to provide robust business solutions and leverage your Java programming.</p> <p>You can deliver HTML5 dynamic scalable applications for desktops, tablets, and smartphones.</p> <p>You can be more productive. The simplified application architecture reduces the amount of boilerplate code needed for business logic.</p> <p>And you can support more enterprise demands. You can write batch applications in Java that use a standard API and are portable across multiple runtimes. You also can break down batch jobs into manageable chunks for uninterrupted performance.</p>	<p>Show animation that describes Java EE 7 and illustrates its main benefits:</p> <ul style="list-style-type: none"> <li>• HTML5 dynamic scalable applications</li> <li>• Increased developer productivity</li> <li>• Enterprise technologies such as batch processing</li> </ul>

Table 67. Grouping of specifications into “Java EE 7 full platform” and “Java EE 7 Web Profile”. Show what specifications are available in the “Java EE 7 full platform” and “Java EE 7 Web Profile” groups.

Scene	Audio	Onscreen Action
3	Java EE 7 introduces the full platform. All Java EE 7 specifications (or JSRs) are in the full platform.	Show image that has the entire Java EE 7. Highlight “Full Platform” and then all specifications.

Table 67. Grouping of specifications into "Java EE 7 full platform" and "Java EE 7 Web Profile" (continued). Show what specifications are available in the "Java EE 7 full platform" and "Java EE 7 Web Profile" groups.

Scene	Audio	Onscreen Action																																																															
4	<p>Specifications for web applications are in the Web Profile, a subset of the full platform.</p> <p>Java EE 6 introduced Web Profile to assist developers of dynamic web applications, providing technologies such as EJB Lite, Java Persistence API, and Java Transaction API.</p> <p>For Java EE 7, Web Profile adds support for HTML5.</p> <p>Two new technologies, WebSocket and JSON, speed up data exchanges and simplify data parsing for portable applications. Updates to existing technologies, JAX-RS 2.0, Java Server Faces 2.2, and Servlet 3.1 enhance your ability to develop dynamic HTML5 applications.</p> <p>A more robust POJO development model enables broader use of annotations, such as in Interceptors and CDI. Bean Validation 1.1 offers method-level validation.</p>	<p>Show image that has the entire Java EE 7. Then show animation that lists the specifications in Web Profile and highlights the specifications named in the audio.</p> <p>Web Profile</p> <table border="1"> <thead> <tr> <th>Specification</th> <th>Java EE 6</th> <th>Java EE 7</th> </tr> </thead> <tbody> <tr><td>Bean Validation</td><td>1.0</td><td>1.1</td></tr> <tr><td>Common Annotations for the Java Platform</td><td>1.1</td><td>1.2</td></tr> <tr><td>Contexts and Dependency Injection (CDI)</td><td>1.0</td><td>1.2</td></tr> <tr><td>Debugging Support for Other Languages</td><td>1.0</td><td>1.0</td></tr> <tr><td>Dependency Injection for Java</td><td>1.0</td><td>1.0</td></tr> <tr><td>Enterprise JavaBeans (EJB) Lite</td><td>3.1</td><td>3.2</td></tr> <tr><td>Expression Language (JSP/EL)</td><td>2.2</td><td>3.0</td></tr> <tr><td>Interceptors</td><td>1.1</td><td>1.2</td></tr> <tr><td>Java API for JSON Processing (JSON-P)</td><td>n/a</td><td>1.0</td></tr> <tr><td>Java API for RESTful Web Services (JAX-RS)</td><td>n/a</td><td>2.0</td></tr> <tr><td>Java Database Connectivity (JDBC)</td><td>4.0</td><td>4.1</td></tr> <tr><td>Java Naming and Directory Interface (JNDI)</td><td>1.0</td><td>1.0</td></tr> <tr><td>Java Servlet</td><td>3.0</td><td>3.1</td></tr> <tr><td>JavaServer Faces (JSF)</td><td>2.0</td><td>2.2</td></tr> <tr><td>JavaServer Pages (JSP)</td><td>2.2</td><td>2.3</td></tr> <tr><td>Java Transaction API (JTA)</td><td>1.1</td><td>1.2</td></tr> <tr><td>Java Persistence API (JPA)</td><td>2.0</td><td>2.1</td></tr> <tr><td>Managed Beans</td><td>1.0</td><td>1.0</td></tr> <tr><td>Standard Tag Library for JavaServer Pages (JSTL)</td><td>1.2</td><td>1.2</td></tr> <tr><td>WebSocket</td><td>n/a</td><td>1.0, 1.1</td></tr> </tbody> </table>	Specification	Java EE 6	Java EE 7	Bean Validation	1.0	1.1	Common Annotations for the Java Platform	1.1	1.2	Contexts and Dependency Injection (CDI)	1.0	1.2	Debugging Support for Other Languages	1.0	1.0	Dependency Injection for Java	1.0	1.0	Enterprise JavaBeans (EJB) Lite	3.1	3.2	Expression Language (JSP/EL)	2.2	3.0	Interceptors	1.1	1.2	Java API for JSON Processing (JSON-P)	n/a	1.0	Java API for RESTful Web Services (JAX-RS)	n/a	2.0	Java Database Connectivity (JDBC)	4.0	4.1	Java Naming and Directory Interface (JNDI)	1.0	1.0	Java Servlet	3.0	3.1	JavaServer Faces (JSF)	2.0	2.2	JavaServer Pages (JSP)	2.2	2.3	Java Transaction API (JTA)	1.1	1.2	Java Persistence API (JPA)	2.0	2.1	Managed Beans	1.0	1.0	Standard Tag Library for JavaServer Pages (JSTL)	1.2	1.2	WebSocket	n/a	1.0, 1.1
Specification	Java EE 6	Java EE 7																																																															
Bean Validation	1.0	1.1																																																															
Common Annotations for the Java Platform	1.1	1.2																																																															
Contexts and Dependency Injection (CDI)	1.0	1.2																																																															
Debugging Support for Other Languages	1.0	1.0																																																															
Dependency Injection for Java	1.0	1.0																																																															
Enterprise JavaBeans (EJB) Lite	3.1	3.2																																																															
Expression Language (JSP/EL)	2.2	3.0																																																															
Interceptors	1.1	1.2																																																															
Java API for JSON Processing (JSON-P)	n/a	1.0																																																															
Java API for RESTful Web Services (JAX-RS)	n/a	2.0																																																															
Java Database Connectivity (JDBC)	4.0	4.1																																																															
Java Naming and Directory Interface (JNDI)	1.0	1.0																																																															
Java Servlet	3.0	3.1																																																															
JavaServer Faces (JSF)	2.0	2.2																																																															
JavaServer Pages (JSP)	2.2	2.3																																																															
Java Transaction API (JTA)	1.1	1.2																																																															
Java Persistence API (JPA)	2.0	2.1																																																															
Managed Beans	1.0	1.0																																																															
Standard Tag Library for JavaServer Pages (JSTL)	1.2	1.2																																																															
WebSocket	n/a	1.0, 1.1																																																															

Table 67. Grouping of specifications into "Java EE 7 full platform" and "Java EE 7 Web Profile" (continued). Show what specifications are available in the "Java EE 7 full platform" and "Java EE 7 Web Profile" groups.

Scene	Audio	Onscreen Action																																																																																																																											
5	<p>Also added for Version 7 are specifications for enterprise, web service, batch and other applications, as well as support for application security, deployment and management. These specifications are in the full platform.</p> <p>Java EE 7 has a simplified architecture requiring less boilerplate code for business logic, such as in JMS 2.0.</p> <p>For the enterprise, you can use Batch Applications to better utilize computing resources by shifting processing times to when resources are typically idle. Concurrency Utilities supports scalable applications that integrate with the Java EE runtime in a secure, reliable manner.</p> <p>The full platform also has updated support for Java Connector Architecture and Java Message Service.</p>	<p>Show image that has the entire Java EE 7. Then show animation that lists the specifications in the full platform and highlights the specifications named in the audio.</p> <p>Full Platform</p> <p>Web Profile</p> <table border="1"> <thead> <tr> <th>Specification</th> <th>Java EE 6</th> <th>Java EE 7</th> </tr> </thead> <tbody> <tr><td>Bean Validation</td><td>1.0</td><td>1.1</td></tr> <tr><td>Common Annotations for the Java Platform</td><td>1.1</td><td>1.2</td></tr> <tr><td>Contexts and Dependency Injection (CDI)</td><td>1.0</td><td>1.2</td></tr> <tr><td>Debugging Support for Other Languages</td><td>1.0</td><td>1.0</td></tr> <tr><td>Dependency Injection for Java</td><td>1.0</td><td>1.0</td></tr> <tr><td>Enterprise JavaBeans (EJB) Lite</td><td>3.1</td><td>3.2</td></tr> <tr><td>Expression Language (JSP/EL)</td><td>2.2</td><td>3.0</td></tr> <tr><td>Interceptors</td><td>1.1</td><td>1.2</td></tr> <tr><td>Java API for JSON Processing (JSON-P)</td><td>n/a</td><td>1.0</td></tr> <tr><td>Java API for RESTful Web Services (JAX-RS)</td><td>n/a</td><td>2.0</td></tr> <tr><td>Java Database Connectivity (JDBC)</td><td>4.0</td><td>4.1</td></tr> <tr><td>Java Naming and Directory Interface (JNDI)</td><td>1.0</td><td>1.0</td></tr> <tr><td>Java Servlet</td><td>3.0</td><td>3.1</td></tr> <tr><td>JavaServer Faces (JSF)</td><td>2.0</td><td>2.2</td></tr> <tr><td>JavaServer Pages (JSP)</td><td>2.2</td><td>2.3</td></tr> <tr><td>Java Transaction API (JTA)</td><td>1.1</td><td>1.2</td></tr> <tr><td>Java Persistence API (JPA)</td><td>2.0</td><td>2.1</td></tr> <tr><td>Managed Beans</td><td>1.0</td><td>1.0</td></tr> <tr><td>Standard Tag Library for JavaServer Pages (JSTL)</td><td>1.2</td><td>1.2</td></tr> <tr><td>WebSocket</td><td>n/a</td><td>1.0, 1.1</td></tr> </tbody> </table> <p>Remaining Full Platform</p> <table border="1"> <tbody> <tr><td>Batch Applications for Java Platform</td><td>n/a</td><td>1.0</td></tr> <tr><td>EE Concurrency Utilities</td><td>n/a</td><td>1.0</td></tr> <tr><td>Enterprise JavaBeans (EJB) full</td><td>n/a</td><td>3.2</td></tr> <tr><td>Implementing Enterprise Web Services</td><td>n/a</td><td>1.4</td></tr> <tr><td>J2EE Management</td><td>n/a</td><td>1.1</td></tr> <tr><td>Java API for RESTful Web Services (JAX-RS)</td><td>1.1</td><td>n/a</td></tr> <tr><td>Java API for XML-Based Web Services (JAX-WS)</td><td>n/a</td><td>2.2</td></tr> <tr><td>Java API for WSDL (JWSDL)</td><td></td><td></td></tr> <tr><td>Java API for XML Processing (JAXP)</td><td>n/a</td><td>1.4</td></tr> <tr><td>Java Architecture for XML Binding (JAXB)</td><td>n/a</td><td>2.2</td></tr> <tr><td>Java Authentication Service Provider Interface for Containers (JASPIC)</td><td>n/a</td><td>1.1</td></tr> <tr><td>Java Authorization Contract for Containers (JACC)</td><td>n/a</td><td>1.5</td></tr> <tr><td>Java EE Connector Architecture (JCA)</td><td>1.6</td><td>1.7</td></tr> <tr><td>JavaMail</td><td>n/a</td><td>1.5</td></tr> <tr><td>Java Message Service (JMS) API</td><td>1.1</td><td>2.0</td></tr> <tr><td>Java Management Extensions (JMX)</td><td>n/a</td><td>2.0</td></tr> <tr><td>JavaBeans Activation Framework (JAF)</td><td>n/a</td><td>1.1</td></tr> <tr><td>SOAP with Attachments API for Java (SAAJ)</td><td>n/a</td><td>1.3</td></tr> <tr><td>Streaming API for XML (StAX)</td><td>n/a</td><td>1.0</td></tr> <tr><td>Web Services Metadata for the Java Platform</td><td></td><td></td></tr> </tbody> </table>	Specification	Java EE 6	Java EE 7	Bean Validation	1.0	1.1	Common Annotations for the Java Platform	1.1	1.2	Contexts and Dependency Injection (CDI)	1.0	1.2	Debugging Support for Other Languages	1.0	1.0	Dependency Injection for Java	1.0	1.0	Enterprise JavaBeans (EJB) Lite	3.1	3.2	Expression Language (JSP/EL)	2.2	3.0	Interceptors	1.1	1.2	Java API for JSON Processing (JSON-P)	n/a	1.0	Java API for RESTful Web Services (JAX-RS)	n/a	2.0	Java Database Connectivity (JDBC)	4.0	4.1	Java Naming and Directory Interface (JNDI)	1.0	1.0	Java Servlet	3.0	3.1	JavaServer Faces (JSF)	2.0	2.2	JavaServer Pages (JSP)	2.2	2.3	Java Transaction API (JTA)	1.1	1.2	Java Persistence API (JPA)	2.0	2.1	Managed Beans	1.0	1.0	Standard Tag Library for JavaServer Pages (JSTL)	1.2	1.2	WebSocket	n/a	1.0, 1.1	Batch Applications for Java Platform	n/a	1.0	EE Concurrency Utilities	n/a	1.0	Enterprise JavaBeans (EJB) full	n/a	3.2	Implementing Enterprise Web Services	n/a	1.4	J2EE Management	n/a	1.1	Java API for RESTful Web Services (JAX-RS)	1.1	n/a	Java API for XML-Based Web Services (JAX-WS)	n/a	2.2	Java API for WSDL (JWSDL)			Java API for XML Processing (JAXP)	n/a	1.4	Java Architecture for XML Binding (JAXB)	n/a	2.2	Java Authentication Service Provider Interface for Containers (JASPIC)	n/a	1.1	Java Authorization Contract for Containers (JACC)	n/a	1.5	Java EE Connector Architecture (JCA)	1.6	1.7	JavaMail	n/a	1.5	Java Message Service (JMS) API	1.1	2.0	Java Management Extensions (JMX)	n/a	2.0	JavaBeans Activation Framework (JAF)	n/a	1.1	SOAP with Attachments API for Java (SAAJ)	n/a	1.3	Streaming API for XML (StAX)	n/a	1.0	Web Services Metadata for the Java Platform		
Specification	Java EE 6	Java EE 7																																																																																																																											
Bean Validation	1.0	1.1																																																																																																																											
Common Annotations for the Java Platform	1.1	1.2																																																																																																																											
Contexts and Dependency Injection (CDI)	1.0	1.2																																																																																																																											
Debugging Support for Other Languages	1.0	1.0																																																																																																																											
Dependency Injection for Java	1.0	1.0																																																																																																																											
Enterprise JavaBeans (EJB) Lite	3.1	3.2																																																																																																																											
Expression Language (JSP/EL)	2.2	3.0																																																																																																																											
Interceptors	1.1	1.2																																																																																																																											
Java API for JSON Processing (JSON-P)	n/a	1.0																																																																																																																											
Java API for RESTful Web Services (JAX-RS)	n/a	2.0																																																																																																																											
Java Database Connectivity (JDBC)	4.0	4.1																																																																																																																											
Java Naming and Directory Interface (JNDI)	1.0	1.0																																																																																																																											
Java Servlet	3.0	3.1																																																																																																																											
JavaServer Faces (JSF)	2.0	2.2																																																																																																																											
JavaServer Pages (JSP)	2.2	2.3																																																																																																																											
Java Transaction API (JTA)	1.1	1.2																																																																																																																											
Java Persistence API (JPA)	2.0	2.1																																																																																																																											
Managed Beans	1.0	1.0																																																																																																																											
Standard Tag Library for JavaServer Pages (JSTL)	1.2	1.2																																																																																																																											
WebSocket	n/a	1.0, 1.1																																																																																																																											
Batch Applications for Java Platform	n/a	1.0																																																																																																																											
EE Concurrency Utilities	n/a	1.0																																																																																																																											
Enterprise JavaBeans (EJB) full	n/a	3.2																																																																																																																											
Implementing Enterprise Web Services	n/a	1.4																																																																																																																											
J2EE Management	n/a	1.1																																																																																																																											
Java API for RESTful Web Services (JAX-RS)	1.1	n/a																																																																																																																											
Java API for XML-Based Web Services (JAX-WS)	n/a	2.2																																																																																																																											
Java API for WSDL (JWSDL)																																																																																																																													
Java API for XML Processing (JAXP)	n/a	1.4																																																																																																																											
Java Architecture for XML Binding (JAXB)	n/a	2.2																																																																																																																											
Java Authentication Service Provider Interface for Containers (JASPIC)	n/a	1.1																																																																																																																											
Java Authorization Contract for Containers (JACC)	n/a	1.5																																																																																																																											
Java EE Connector Architecture (JCA)	1.6	1.7																																																																																																																											
JavaMail	n/a	1.5																																																																																																																											
Java Message Service (JMS) API	1.1	2.0																																																																																																																											
Java Management Extensions (JMX)	n/a	2.0																																																																																																																											
JavaBeans Activation Framework (JAF)	n/a	1.1																																																																																																																											
SOAP with Attachments API for Java (SAAJ)	n/a	1.3																																																																																																																											
Streaming API for XML (StAX)	n/a	1.0																																																																																																																											
Web Services Metadata for the Java Platform																																																																																																																													

Table 67. Grouping of specifications into "Java EE 7 full platform" and "Java EE 7 Web Profile" (continued). Show what specifications are available in the "Java EE 7 full platform" and "Java EE 7 Web Profile" groups.

Scene	Audio	Onscreen Action
6	<p>In all, Java EE 7 has over 20 new or changed specifications.</p> <p>The Liberty product supports the full platform specifications, while the Liberty Core product supports mainly the Web Profile specifications.</p>	Show image of the entire Java EE 7. Highlight the specifications supported by Liberty and then Liberty Core.

Table 68. Demo installing Liberty with Java EE 7 by extracting a compressed (ZIP) file. Show how to install a Liberty runtime with Java EE 7 by extracting a ZIP file downloaded from WASdev.

Scene	Audio	Onscreen Action
7	You can install Liberty with Java EE 7 technologies by downloading a compressed, or ZIP, file from the WASdev website to a temporary directory, and then extracting the ZIP file to an empty directory.	Show how to download a ZIP file with Liberty and Java EE technologies from the WASdev website to C:\wlp_temp on a workstation and then extract the ZIP file to C:\, resulting in installation of Liberty to C:\wlp.
8	It's that simple!	Show selecting the C:\wlp installation directory.

Table 69. Demo adding a Liberty runtime with Java EE 7 features in WebSphere Developer Tools for Eclipse. Show how to install a server with Java EE features in WebSphere Developer Tools.

Scene	Audio	Onscreen Action
9	<p>In WebSphere Developer Tools for Eclipse, you can add a Liberty runtime with Java EE technologies.</p> <p>Create a new server and select to download and install a Liberty runtime environment from <a href="http://ibm.com">ibm.com</a>.</p> <p>The runtime options with Java EE 7 technologies are for the full platform, Web Profile or client.</p> <p>You can add on individual features. Technologies that are in the selected runtime option are greyed out.</p>	<p>Show images that demo how to add a Liberty server that has Java EE technologies in WebSphere Developer Tools.</p> <ol style="list-style-type: none"> <li>1. Right-click in the Servers view and select <b>New &gt; Server</b>.</li> <li>2. In the New Server wizard: <ol style="list-style-type: none"> <li>a. Select the <b>WebSphere Application Server Liberty</b> server type and click the <b>Add</b> link.</li> <li>b. Select <b>Install from an archive or repository</b> and click <b>Next</b>.</li> <li>c. Specify the location to which to install Liberty, select <b>Download and install a new runtime environment from ibm.com</b>, select a Liberty product with Java EE 7 technologies, and click <b>Next</b>.</li> <li>d. Select any add-ons to install and click <b>Next</b>.</li> <li>e. Accept the license agreement and click <b>Finish</b>.</li> <li>f. After installation, click <b>Next</b>.</li> <li>g. Specify a server name and click <b>Next</b>.</li> <li>h. Click <b>Finish</b>.</li> </ol> </li> </ol> <p>To start the server, right-click the Liberty server in the Servers view and click <b>Start</b>.</p>

Table 70. Demo adding Java EE 7 features to a Liberty installation from a command line and Installation Manager. Show how to run an `installUtility` command to install Java EE features. Briefly show the Installation Manager option.

Scene	Audio	Onscreen Action
10	If you already have Liberty installed, you can add Java EE 7 features to your installation by running a <code>featureManager</code> or <code>installUtility</code> command.	Show running an <code>installUtility</code> command to install features into an existing installation of Liberty at C:\wlp. <ol style="list-style-type: none"> <li>From a command line at C:\wlp\bin, show running a command to install the <code>webProfile-7.0</code> feature:  <pre>installUtility install webProfile-7.0</pre> </li> <li>Enter 1 to agree to the terms of the license agreement.</li> </ol> <p>Command messages list the features installed.</p>
11	You also can use Installation Manager to install Java EE 7 features.	Show images that demo how to use Installation Manager to install Liberty with Java EE 7 features. <ol style="list-style-type: none"> <li>During installation of IBM WebSphere Application Server Liberty Network Deployment 8.5.5.6, under <b>Liberty Repositories</b> on the Install Packages page, select <b>Allow Installation Manager to connect to the IBM WebSphere Liberty Repository</b> and click <b>Next</b>.</li> <li>Under <b>Asset Selection</b> on the Install Packages page, click <b>Launch Asset Selection Wizard</b>.</li> <li>In the Asset Selection dialog: <ol style="list-style-type: none"> <li>Click the <b>Install</b> button to select a Java EE technology to install.</li> <li>After the <b>Install</b> button changes to the <b>Install Pending</b> button, click <b>Next</b>.</li> <li>Under <b>License Agreement</b>, select <b>I accept the terms in the license agreement</b> and click <b>Finish</b>.</li> </ol> </li> <li>Under <b>Asset Selection</b> on the Install Packages page, review the list of assets to install and click <b>Next</b>.</li> </ol>
12		Show a summary of the ways to install Java EE 7 technologies for Liberty: <ul style="list-style-type: none"> <li>ZIP file from the WASdev website</li> <li>WebSphere Application Server Developer Tools for Eclipse</li> <li><code>installUtility</code> or <code>featureManager</code> command</li> <li>IBM Installation Manager</li> </ul>

Table 71. Demo configuration of a Liberty server to add a Java EE 7 feature. Show how to add a Java EE 7 feature to a server configuration.

Scene	Audio	Onscreen Action
13	After Java EE 7 features are installed, adding support for a Java EE 7 specification to a Liberty server is as simple as adding a feature name to a <code>server.xml</code> file.	Under the heading <i>Configuration</i> , show a command line at C:\wlp\bin with the command <code>server run server1</code> and with messages indicating that <code>server1</code> is running. Also show a text editor open on the <code>server.xml</code> file of <code>server1</code> . Finally, show adding the <code>jaxrs-2.0</code> feature to a feature manager and the resulting <code>server1</code> messages that confirm the server configuration change.
14	Liberty provides the <code>javaee-7.0</code> , <code>webProfile-7.0</code> , and <code>javaeeClient-7.0</code> convenience features to make it easier to enable your servers to support a broad range of applications.	Show a list of the Liberty convenience features for Java EE 7: <ul style="list-style-type: none"> <li><code>javaee-7.0</code></li> <li><code>webProfile-7.0</code></li> <li><code>javaeeClient-7.0</code></li> </ul>

Table 71. Demo configuration of a Liberty server to add a Java EE 7 feature (continued). Show how to add a Java EE 7 feature to a server configuration.

Scene	Audio	Onscreen Action
15	Use the <code>javaee-7.0</code> feature to quickly add support for all specifications. The <code>webProfile-7.0</code> feature adds support for web applications. And the <code>javaeeClient-7.0</code> feature allows you to quickly configure an application client component.	Show sample configuration files for the <code>javaee-7.0</code> , <code>webProfile-7.0</code> , and <code>javaeeClient-7.0</code> convenience features.

Table 72. Some features require configuration or migration. Show where to find instructions about the needed configuration or migration.

Scene	Audio	Onscreen Action
16	<p>The IBM Knowledge Center has information about the features.</p> <p><i>Java EE 7 programming model support</i> lists the Java EE specifications, provides links to the JSRs and Liberty features, and tells you what products support the specifications. Note that not all Java EE specifications have their own Liberty feature.</p> <p>For some of the features, you'll need to do configuration beyond adding the feature name to a <code>server.xml</code>.</p> <p>If your server uses Java EE 6 features and you are considering adding Version 7 features, look at <i>Supported Java EE 6 and 7 feature combinations</i>. Also, look at <i>Java EE 7 behavior changes</i> to see whether moving from a Version 6 feature to a Version 7 feature would benefit your applications and environment.</p> <p>For details on features, see <i>Liberty features</i>.</p>	<p>Show topics in Knowledge Center that identify and cover feature configuration and migration:</p> <ul style="list-style-type: none"> <li>• <i>Java EE 7 programming model support</i></li> <li>• <i>Supported Java EE 6 and 7 feature combinations</i></li> <li>• <i>Java EE 7 behavior changes</i></li> <li>• <i>Liberty features</i></li> </ul>

Table 73. Conclusion. Show where to find more information about Java EE 7 in Liberty.

Scene	Audio	Onscreen Action
17	For how-to articles and videos on using Java EE 7 in your applications as well as information about configuring servers, see <code>WASdev.net</code> and the WebSphere Application Server Liberty documentation on IBM Knowledge Center.	<p>Show where to find information about Java EE 7 in Liberty:</p> <p><b>WASdev</b>  <a href="http://developer.ibm.com/wasdev">http://developer.ibm.com/wasdev</a></p> <p><b>IBM Knowledge Center</b>  <a href="http://www.ibm.com/support/knowledgecenter/">http://www.ibm.com/support/knowledgecenter/</a></p>

For more information, see “Java EE 7 in Liberty” on page 4.

## Video: OpenID Connect on Liberty

8.5.5.5

The following transcript is for the “OpenID Connect on Liberty” video, which demonstrates how to configure OpenID Connect on Liberty. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content that is shown in the video.

## OpenID Connect on Liberty

*Table 74. Title page.* Show title and then a basic OpenID Connect scenario, along with supported OpenID providers and benefits of using OpenID Connect.

Scene	Audio	Onscreen Action
1	This video will show you how to set up a simple OpenID Connect web single-sign-on scenario using WebSphere Application Server Liberty.	Show title <i>OpenID Connect Quick Setup</i> .
2	<p>Here you can see a basic "OpenID Connect" flow. When a user first attempts to access an OpenID Connect-protected web application, or relying party, the user is redirected to an OpenID Connect provider. The OpenID Connect provider authenticates the user and obtains the user's authorization, then responds with an authorization code. The application container then extracts the code from the response, sends the code back to the OpenID provider for verification, and receives ID and access tokens. As a result, the user is authenticated to access the protected web application. Using the access token, the application can request user information, such as an email address, from the OpenID Connect provider, or it can access any service that supports OpenID Connect. In this video, I will refer to the application as the "Relying Party" or RP and the "OpenID Provider" as OP.</p> <p>Let's take a look at the several supported OpenID providers.</p>	Show a basic OpenID Connect scenario, that includes a Relying Party (RP), OpenID Provider (OP), and an End-User.
3	You can configure IBM WebSphere Liberty either as an OpenID provider or a relying party. You can use IBM Security Access Manager, also known as ISAM, as an OP as well. Alternatively, you can use a number of supported third-party OpenID providers.	Show some of the supported OpenID providers. <ul style="list-style-type: none"><li>• IBM WebSphere</li><li>• IBM Security Access Manager</li><li>• Amazon</li><li>• Microsoft</li><li>• Okta</li><li>• Google</li></ul>

Table 74. Title page (continued). Show title and then a basic OpenID Connect scenario, along with supported OpenID providers and benefits of using OpenID Connect.

Scene	Audio	Onscreen Action
4	<p>OpenID Connect offers a number of benefits as an identity layer on top of OAUTH 2.0. With OpenID Connect, users have a single internet identity that they can use to authenticate across several servers, services, and applications, and it reduces the amount of maintenance work in applications because they no longer need their own user registry.</p> <p>For developers, it simplifies the task of authenticating users without taking on the responsibility of storing and managing passwords. OpenID Connect can also extend security services to cloud-based and mobile applications written in any language, such as JavaScript, Ruby, node.js, or Java, and it can function as a single security manager for provisioning hundreds of Liberty servers in a cloud environment. Because OpenID Connect combines the advantages of identity, authentication, and OAuth, OpenID Connect is a significant improvement over OAuth alone.</p>	<p>Show some of the benefits of using OpenID Connect.</p> <ul style="list-style-type: none"> <li>• OpenID Connect makes it easier for a user to use a single internet identity (user account), to authenticate across several servers, services, and applications.</li> <li>• Applications no longer need to maintain their own user registry.</li> <li>• OpenID Connect extends security services to cloud and mobile applications, accessible through languages such as JavaScript, Ruby, node.js, Java</li> <li>• Provisioning hundreds of Liberty servers in a cloud offers the ability to have a single security manager</li> <li>• OpenID Connect is a significant improvement over OAUTH 2.0</li> </ul>

Table 75. Demo configuring the OpenID Provider

Scene	Audio	Onscreen Action
5	<p>WebSphere Application Server Liberty can be configured as the OpenID provider, the relying party, or both. If you want to use Liberty as both an OP and RP, you must configure them on different Liberty server instances. We will set up Liberty servers as OP and RP and take a look at a simple web single-sign-on scenario between the Liberty OP and RP.</p>	<p>Show title <i>Setting up Liberty as OpenID Connect provider and relying party.</i></p>
6	<p>First, we will set up an OpenID provider.</p> <p>To do so, we will install WebSphere Liberty 8554 or later, which is required to use the OpenID Connect features. Install the OpenID Server feature</p> <p>Create a Liberty server and add an OP configuration to the server.xml file, which is available as a downloadable sample from IBM developerWorks.</p>	<p>Show OP setup overview.</p> <ol style="list-style-type: none"> <li>1. Install WebSphere Liberty 8.5.5.4 or above &gt; <b>java -jar wlp-developers-runtime-8.5.5.4.jar</b></li> <li>2. Install OpenID Server feature (No download necessary) &gt; <b>bin/featureManager install openidConnectServer-1.0 --when-file-exists=ignore</b></li> <li>3. Create a Liberty server &gt; <b>server create oidcServer</b></li> </ol> <ul style="list-style-type: none"> <li>• Edit server.xml with more configurations (Sample downloadable)</li> <li>• Required features</li> <li>• SSL keystore</li> <li>• User Registry</li> <li>• OpenID Server</li> </ul>

Table 75. Demo configuring the OpenID Provider (continued)

Scene	Audio	Onscreen Action
7	<p>First, unpack the Liberty JAR file. This creates the wlp directory. Go to the bin directory under wlp, and run the <b>featureManager install</b> command to install the OpenID Connect Server feature.</p> <p>In the same directory, run the <b>server create</b> command to create a Liberty OP server. We will name this one oidcServer.</p> <p>oidcServer is now created with the minimum configuration in the server.xml file. You can find the configuration in the wlp/usr/server/oidcServer directory.</p> <p>Here you can see the contents of the server.xml file that we just created. The configuration is very simple, just one feature and port information. We will replace it with a server.xml file that has the OP server configuration. (Screen splits and right-hand side OP config appears).</p> <p>(Going through updates in the server.xml file) In this OP server configuration,</p> <ul style="list-style-type: none"> <li>• Required features are added.</li> <li>• A host name is added.</li> <li>• Keystore configuration is included for the SSL feature.</li> <li>• The OP maintains user accounts, so a user registry is configured.</li> </ul> <p>The rest is OP configuration that uses OAuth technology. It includes information about the relying party that it performs authorization for.</p> <p>You can download the server.xml file that we just added from IBM DeveloperWorks. We will start the OP server. Now that we have set up the OpenID provider, we can set up the Liberty relying party.</p>	<p>Demo with a command prompt that is being used to update server.xml file.</p>

Table 76. Demo configuring the Relying Party

Scene	Audio	Onscreen Action
8	<p>To set up the relying party, just like the OP configuration, we need to have version 8.5.5.4 or later of the Liberty profile and we will install the OpenID Client feature.</p> <p>We will create a separate Liberty server and edit the server.xml file.</p> <p>Then we will install the application and exchange keys with the OpenID provider for SSL communication.</p>	<p>Show RP setup overview.</p> <ol style="list-style-type: none"> <li>1. Install WebSphere Liberty 8.5.5.4 &gt; <b>java -jar wlp-developers-runtime-8.5.5.4.jar</b></li> <li>2. Install OpenID Client feature (No download necessary) &gt; <b>bin/featureManager install openidConnectClient-1.0 --when-file-exists=ignore</b></li> <li>3. Create a Liberty server &gt; <b>server create oidcRP</b> <ul style="list-style-type: none"> <li>• Edit server.xml with more configurations (Sample downloadable)</li> <li>• Required features</li> <li>• SSL keystore</li> <li>• OpenID Client</li> <li>• Application</li> </ul> </li> </ol> <ol style="list-style-type: none"> <li>1. Install application (that uses OpenID Connect) &gt;&gt; Copy application ear/war file under app directory <ul style="list-style-type: none"> <li>• Exchange keys with OP for SSL communication</li> </ul> </li> </ol>
9	<p>Version 8.5.5.4 of Liberty is already configured on this machine. We will install the OpenID Client feature and create a server with the name oidcRP. Here is the default server.xml file. Now, we will compare it to a server.xml file with an RP configuration. These sections - features, endpoint host name, keystores - are the same updates that we previously saw with the OP.</p> <p>This time, we have an OpenID Client configuration instead of the OP server configuration. It specifies the OP URLs to send authentication requests to.</p> <p>The RP configuration also includes application configuration and these applications rely on the OP to perform authentication.</p> <p>Note that there is no user registry configuration on the RP. That is all the configuration needed for the RP. We will copy a test application into the app directory of the RP. Before you start the RP server, make sure that the RP and OP exchanged the keys in the keystore for SSL communication. In this demo, we will use the same keystore and same password.</p> <p>Now we will start the RP server to see if we are set up correctly.</p>	<p>Demo with a command prompt that is being used to update server.xml file.</p>

Table 77. Demo testing the OP/RP setup

Scene	Audio	Onscreen Action
10	The OP and RP servers are already started. In a browser, we will go to the application URL. When prompted, we will enter account information from the OP. We will see the RP relying on the OP to perform authentication. Once the user is authenticated, the RP will show an application page to the user. Let's try that now.	<p>Demo testing the OP/RP setup.</p> <ol style="list-style-type: none"> <li>1. Start both OP and RP servers, &gt; <b>server start oidcServer</b> &gt; <b>server start oidcRP</b></li> <li>2. In a browser, point to the application login page on RP &gt; <a href="https://oidc-rp.rtp.raleigh.ibm.com:9443/testpage">https://oidc-rp.rtp.raleigh.ibm.com:9443/testpage</a></li> <li>3. When prompted, enter the user ID and password that is maintained by the OP &gt; user1 / security</li> <li>4. RP relies on OP for authentication</li> <li>5. Upon successful authentication, RP serves application page with user information.</li> </ol>
11	<p>In the browser, we will type in the application URL that is on the RP server. It will prompt for a user name and password. Notice that we are being prompted by the OP server because the RP is delegating the authentication to the OP.</p> <p>We will enter user1 and security, which are the credentials for the OP account. Now we are successfully logged in to the application on the RP using the OP account.</p>	<p>Demo with a browser login that shows a successful login into the application on the RP that is using the OP account.</p>

Table 78. Conclusion. Show where to find more information about OpenID Connect.

Scene	Audio	Onscreen Action
12	For more information, visit these online resources.	<p>Show information on documentation:</p> <p><b>WebSphere Liberty download page</b>  <a href="https://developer.ibm.com/wasdev/downloads/liberty-profile-using-non-eclipse-environments/">https://developer.ibm.com/wasdev/downloads/liberty-profile-using-non-eclipse-environments/</a></p> <p><b>OpenID Connect feature installation</b>            Server: <a href="https://developer.ibm.com/wasdev/downloads/#asset/features-com.ibm.websphere.appserver.openidConnectServer-1.0">https://developer.ibm.com/wasdev/downloads/#asset/features-com.ibm.websphere.appserver.openidConnectServer-1.0</a>            Client: <a href="https://developer.ibm.com/wasdev/downloads/#asset/features-com.ibm.websphere.appserver.openidConnectClient-1.0">https://developer.ibm.com/wasdev/downloads/#asset/features-com.ibm.websphere.appserver.openidConnectClient-1.0</a></p> <p><b>IBM Knowledge Center - OpenID Connect main page</b>  <a href="http://www-01.ibm.com/support/knowledgecenter/api/content/n1/en-us/SSAW57_8.5.5/com.ibm.websphere.wlp.nd.multipatform.doc/ae/rwlp_using_oidc.html">http://www-01.ibm.com/support/knowledgecenter/api/content/n1/en-us/SSAW57_8.5.5/com.ibm.websphere.wlp.nd.multipatform.doc/ae/rwlp_using_oidc.html</a></p> <p><b>IBM DeveloperWorks (including OP/RP sample)</b>  <a href="http://www.ibm.com/developerworks/websphere/library/techarticles/1502_odonnell/1502_odonnell.html">http://www.ibm.com/developerworks/websphere/library/techarticles/1502_odonnell/1502_odonnell.html</a></p>

For more information about OpenID Connect, see [8.5.5.5](#) Using OpenID Connect.

## Video: Setting up Admin Center



8.5.5.2

The following transcript is for the “Setting up Admin Center” video, which demonstrates how to configure a `server.xml` file to enable Admin Center. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content shown in the video.

### Setting up Admin Center

Table 79. Demo setting up Admin Center in Liberty. Show `server.xml` changes.

Scene	Audio	Onscreen Action
1	This video shows how to enable Liberty Admin Center and get to the login page. Enabling Admin Center is quick and easy.	Show Liberty Admin Center login page in web browser.
2	You need a Liberty Version 8.5.5.2 or later installation. Make a few changes to the <code>server.xml</code> file of a server and you can use the Admin Center.	In Windows Explorer, show <code>wlp/usr</code> Liberty installation directory with no server defined.
3	I have just installed Liberty. To add a server, I go to a command prompt at the <code>wlp/bin</code> directory and run:  <code>server create myServer</code>  This creates a server named <code>myServer</code> .	Show command window open at <code>wlp/bin</code> , run <code>server create myServer</code> , and then show message <code>Server myServer created</code> .
4	The <code>server.xml</code> file is in the <code>usr/servers/myServer</code> directory. I want to make 4 changes to this <code>server.xml</code> file.	In Windows Explorer, select <code>wlp/usr/servers/myServer</code> directory. Select <code>server.xml</code> .
5	First, I add the <code>adminCenter-1.0</code> feature to the feature manager.	In editor open on <code>server.xml</code> , add the <code>adminCenter-1.0</code> feature to the feature manager:  <pre>&lt;featureManager&gt;   &lt;feature&gt;jsp-2.2&lt;/feature&gt;   &lt;feature&gt;adminCenter-1.0&lt;/feature&gt; &lt;/featureManager&gt;</pre>
6	Second, I add a <code>quickStartSecurity</code> element and specify a user name and password to configure a secure login. My user name is <code>admin</code> and my password is <code>adminpwd</code> .	In editor, add user name and password:  <pre>&lt;quickStartSecurity userName="admin"   userPassword="adminpwd" /&gt;</pre>
7	Third, I add a <code>keyStore</code> element to protect keystore files that have server authentication credentials. I choose <code>defaultKeyStore</code> for the <code>id</code> attribute and <code>Liberty</code> for the <code>password</code> attribute.	In editor, add keystore:  <pre>&lt;keyStore id="defaultKeyStore"   password="Liberty" /&gt;</pre>
8	Fourth, I add a <code>host</code> attribute set to asterisk to the <code>httpEndpoint</code> element. Setting <code>host</code> to asterisk, or to a defined host name, lets me view Admin Center on a cell phone, tablet, and remote computer, and not just on this <code>localhost</code> computer.	In editor, press enter after <code>id="defaultHttpEndpoint"</code> in the <code>httpEndpoint</code> element and add <code>host="*"</code> to the new line:  <pre>&lt;httpEndpoint id="defaultHttpEndpoint"   host="*"   httpPort="9080"   httpsPort="9443" /&gt;</pre>
9	Save the <code>server.xml</code> changes.	In editor, save changes.

Table 79. Demo setting up Admin Center in Liberty (continued). Show server.xml changes.

Scene	Audio	Onscreen Action
10	<p>Make these server.xml changes for every Liberty server and collective controller that you want to be able to view in Admin Center.</p> <p>In a multiple-server environment, you only need to make these changes to the server.xml file of a collective controller. You do not need to change the server.xml files of members.</p>	In editor, continue to show server.xml.

Table 80. Displaying Admin Center. Show starting the server, highlighting the adminCenter URL, and pointing a browser at the URL.

Scene	Audio	Onscreen Action
11	<p>I am now ready to start myServer and see Admin Center. Because I want messages shown in the foreground, I use the <b>run</b> command. I enter:</p> <pre>server run myServer</pre> <p>To not show the messages, I would enter:</p> <pre>server start myServer</pre>	In command window on wlp/bin directory, enter server run myServer. The command runs and product messages display in the command window.
12	Liberty writes status messages to the command window. One message has the URL for the adminCenter web application.	Highlight <code>http://host_name:9080/adminCenter/</code> URL in messages.
13	I put this URL into a web browser, and press Enter. The URL changes to https and port 9443 because I specified a secure connection in the server.xml file.	Add URL <code>http://host_name:9080/adminCenter/</code> to browser, press Enter, show URL change to <code>https://host_name:9443/adminCenter/</code> .
14	You might need to add a browser exception to confirm that the connection is trusted.	Show Firefox dialog and button selections <b>Add Exception</b> , <b>Get Certificate</b> , and then <b>Confirm Security Exception</b> .
15	I am now ready to log in to Admin Center.	Show Liberty Admin Center login page.

Table 81. Conclusion. Show where to find more information about Admin Center.

Scene	Audio	Onscreen Action
16	For information on logging into and using Admin Center, and viewing your personal Toolbox, see WASdev.net and the WebSphere Application Server Liberty documentation on IBM Knowledge Center.	<p>Show Liberty Admin Center login page with login fields and title covered by information on documentation:</p> <p><b>WASdev</b>  <a href="http://developer.ibm.com/wasdev">http://developer.ibm.com/wasdev</a></p> <p><b>WebSphere Application Server Liberty documentation on IBM Knowledge Center</b>  <a href="http://www-01.ibm.com/support/knowledgecenter/">http://www-01.ibm.com/support/knowledgecenter/</a></p> <p>Fade the information on documentation and end by showing just the Liberty Admin Center login page.</p>

For more information, see “Administering Liberty using Admin Center” on page 1741.

## Video: Thoughts on Liberty: Interview with Alasdair Nottingham

The following transcript is for the “Thoughts on Liberty: Interview with Alasdair Nottingham ” video. Alasdair shares his perspectives as a lead developer of WebSphere Application Server Liberty on why Liberty is exciting for developers. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content that is shown in the video.

### Thoughts on Liberty: Interview with Alasdair Nottingham

*Table 82. Thoughts on Liberty: Interview with Alasdair Nottingham.* As lead developer for WebSphere Application Server Liberty, Alasdair Nottingham shares his perspectives on Liberty and its value for developers.

Scene	Audio	Onscreen Action
1	None	Show "IBM".
2	None	Show "Liberty".
3	None	Show the text:  Liberty is a new lightweight, easy to use version of WebSphere Application Server. We asked IBM developers to share their thoughts on what it means for developers ...
4	None	Show the question:  What do you find exciting about Liberty?
5	It's this really simple configuration that you can just go and edit with Notepad. I use Unix on a daily basis and being able to go in and edit it kinda completely breaks the expectation that people have of what WebSphere Application Server is. When we say, "Here is what Liberty is," the look of shock and disbelief of people seeing a runtime that starts in seconds, and is dynamic and flexible and has all the behaviors that Liberty has, I think is really exciting.	Show the developer, Alasdair Nottingham, talking on camera. Alasdair Nottingham is a lead developer for WebSphere Application Server Liberty.  Show words: <ul style="list-style-type: none"> <li>• Simple configuration</li> <li>• Breaks expectations</li> <li>• Dynamic</li> <li>• Flexible</li> </ul>
6	None	Show the question:  Tell us about a Liberty user experience?
7	We've got jazz.net which is a website hosting a whole lot of technologies around development. I got contacted one day by the jazz.net lead and he said, "I wanted you to that know we just got into production for our download application on jazz.net." He had not come and spoken to the development team or raised any issues. He had just gone ahead and taken an application that previously had been running elsewhere and got it up and running on jazz.net. All he was talking about what how great an experience it was. He said it was easy to tune and to get it to behave correctly. He was really excited.	Show the developer, Alasdair Nottingham, talking on camera.  Show words: <ul style="list-style-type: none"> <li>• Great experience</li> </ul>
8	None	Show the question:  What would you like to say to developers?

Table 82. *Thoughts on Liberty: Interview with Alasdair Nottingham (continued)*. As lead developer for WebSphere Application Server Liberty, Alasdair Nottingham shares his perspectives on Liberty and its value for developers.

Scene	Audio	Onscreen Action
9	<p>Well I think the important thing is to try it out. An awful lot of people have preconceptions on what proprietary software is like. Or what IBM software is like, in particular. I really think we have tried very hard to learn from the best examples of good usability.</p> <p>We've especially been focused around trying to make it good for developers. At the end of the day, I'm a developer. I work with a bunch of developers and we want to write something that is really good for developers to go and use. I think it really enables you to do a lot of thing that you couldn't do before.</p> <p>It runs in production just as easily. It's completely supported in production environments. That's something that people miss when we say it is a developer focused runtime. It's not to say we aren't trying to provide a runtime for production. It's just saying that by making sure we provide a great developer-friendly runtime, we get a great production-ready runtime at the same time.</p>	<p>Show the developer, Alasdair Nottingham, talking on camera.</p> <p>Show words:</p> <ul style="list-style-type: none"> <li>• Try it out</li> <li>• Good for developers</li> <li>• Completely supported in production</li> </ul>
10	None	<p>Show the text:</p> <p>To learn more: <a href="http://wasdev.net">http://wasdev.net</a></p>

## Video: Touring Admin Center



The following transcript is for the “Touring Admin Center” video, which briefly describes Admin Center features. This transcript is the video storyboard. The video does not have Audio text. Onscreen Action describes the images and words shown.

### Touring Admin Center

Table 83. *Touring Admin Center*. Show images of Admin Center and describe its features in on-screen text.

Scene	Audio	Onscreen Action
1	No narration. Background music.	Show title, <i>Touring Admin Center</i> .
2		Show words <i>Secure login</i> while showing the login page.
3		Show words <i>from a desktop, tablet and smartphone</i> while showing Admin Center login page in a web browser on a desktop monitor, then on a tablet, then on a smartphone.
4		Show words <i>Toolbox</i> and then <i>to hold tools and bookmarks of URLs to favorite websites</i> while showing the Toolbox.
5		Show words <i>customizable by each user</i> while showing Edit Toolbox page, Add Bookmark, and then Add Bookmark dialog.
6		Show words <i>Server Config tool</i> and then <i>to view and edit server.xml and configuration files</i> while showing Server Config tool open on a <i>server.xml</i> file.
7		Show words <i>Explore tool</i> and then <i>to browse applications, clusters, servers and hosts</i> while showing Explore tool Dashboard, then application details page, and then Servers page.

Table 83. *Touring Admin Center (continued).* Show images of Admin Center and describe its features in on-screen text.

Scene	Audio	Onscreen Action
8		Show words <i>to manage resources</i> while showing Start action on two selected resources on Servers page and then search for resources on Search page.
9		Show words <i>to monitor resource metrics</i> while showing charts for a servlet on Monitor page.
10		Show words <i>and to set and view administrative metadata</i> while showing Tags and Metadata dialog and then metadata on server details page.
11		Show words <i>Deploy tool</i> and then <i>to install Liberty server packages on hosts in a collective</i> while showing Deploy tool.
12		Show words <i>Background Tasks</i> and then <i>to check the status of Deploy Installation tasks</i> and then <i>and to view messages</i> while showing Background Tasks page.
13		Show words <i>An interface that informs and guides</i> while showing message for Add Bookmark pop-up dialog.
14		Show words <i>and has preference options</i> while showing Preferences page.

Table 84. *Conclusion.* Show where to get Admin Center.

Scene	Audio	Onscreen Action
15	No narration. Background music.	Show words <i>Available from</i> and then <i>WASdev</i> and <i>http://developer.ibm.com/wasdev</i> .

For more information, see “Administering Liberty using Admin Center” on page 1741.

## Video: Using the IBM WebSphere Liberty Repository to enhance Liberty environments



The following transcript is for the “Using the IBM WebSphere Liberty Repository to enhance Liberty environments” video, which briefly describes the Liberty Repository, its rich set of assets, and how to obtain the assets. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content shown in the video.

### Using the Liberty Repository to enhance Liberty environments

Table 85. *Using the IBM WebSphere Liberty Repository to enhance Liberty environments.* Show images of WASdev.net and other methods of obtaining Liberty features, and describe the Liberty Repository in on-screen text.

Scene	Audio	Onscreen Action
1	Using the IBM WebSphere Liberty Repository to easily enhance your Liberty environment	Show title, <i>Using the IBM WebSphere Liberty Repository to easily enhance your Liberty environment</i> .
2	The rapid evolution and adoption of cloud, mobile, and social media technologies are driving the demand for delivering applications faster and more frequently. IBM WebSphere Application Server is now delivering features for Liberty on a continual basis via the Liberty Repository. In this video, you will learn about the Liberty Repository, its rich set of resources, and how to get started to obtain the latest Liberty features that are available.	Images representing, cloud, mobile, and social media appear. The words “develop applications faster,” “IBM WebSphere Application Server,” “New Liberty features on a continual basis,” and “Liberty Repository” are shown.

Table 85. Using the IBM WebSphere Liberty Repository to enhance Liberty environments (continued). Show images of WASdev.net and other methods of obtaining Liberty features, and describe the Liberty Repository in on-screen text.

Scene	Audio	Onscreen Action
3	Building on the highly composable and modular nature of Liberty, we are making available new features on a continuous basis that you can use to easily extend or enhance your Liberty-based applications. The optional, production-ready features can be quickly and easily added to an existing WebSphere Liberty V8.5.5 installation. Simply choose the features that you want and then install the features to the applicable product service level. The features that you add inherit the same support of your existing installation.	Building blocks representing Liberty features drop down, building a stack of blocks. The word “Optional, production-ready features” and “Add to existing Liberty environment” are shown.
4	Some of the available features include: <ul style="list-style-type: none"> <li>• IBM WebSphere Liberty Administrative Center</li> <li>• IBM WebSphere Liberty Connector Architecture</li> <li>• IBM WebSphere Liberty Optimized Adapters for z/OS</li> <li>• IBM WebSphere Liberty z/OS Connect</li> </ul>	Show words: <ul style="list-style-type: none"> <li>• <i>IBM WebSphere Liberty Administrative Center</i></li> <li>• <i>IBM WebSphere Liberty Connector Architecture</i></li> <li>• <i>IBM WebSphere Liberty Optimized Adapters for z/OS</i></li> <li>• <i>IBM WebSphere Liberty z/OS Connect</i></li> </ul>
5	With the Liberty Repository, you can easily obtain these composable features, as well as enhancements and helpful development tools, from the Repository, rather than having to wait for new product releases. The Liberty Repository enables us to deliver these valuable assets to you faster so that you can more quickly produce, enhance, and deliver innovations and engaging applications.	Show the WASdev Downloads page and the entries for features. Each entry includes an icon, the type of asset, the name of the asset, the release date, a description, and a rating.
6	In addition to features, the repository also includes artifacts such as administration scripts, samples, configuration snippets as well as artifacts that integrate open source projects more quickly and effectively. These assets are specifically designed to encompass end-to-end integration and provide important business value for the entire life-cycle of your Liberty application.	Show the WASdev Downloads page and the entries for other assets on the page. Each entry includes an icon, the type of asset, the name of the asset, the release date, a description, and a rating.  Show a list of all possible asset types and their associated icons: <ul style="list-style-type: none"> <li>• Features</li> <li>• Product samples</li> <li>• Addons</li> <li>• Product runtimes</li> <li>• Admin scripts</li> <li>• Config snippets</li> <li>• Open source integration</li> <li>• Tools</li> </ul>
7	To get started, visit WASdev.net from your computer or mobile device. From the home page, click Downloads to browse and discover the variety of assets in the repository. You can search to find the assets you need. Also, you can use filtering to scope your search by asset type and edition. From WASdev.net, you can learn about the available features and how to install them using product installation tools, WebSphere Developer Tools or Rational® Application Developer.	Show the WASdev.net homepage. The cursor clicks on <b>Downloads</b> and scrolls through the asset listing. “MongoDB” is searched for, then the cursor clicks on the <b>Filter</b> menu and clicks <b>Feature</b> to filter the results to show only features.

Table 85. Using the IBM WebSphere Liberty Repository to enhance Liberty environments (continued). Show images of WASdev.net and other methods of obtaining Liberty features, and describe the Liberty Repository in on-screen text.

Scene	Audio	Onscreen Action
8	The Liberty Repository has been seamlessly integrated with the Liberty installation methods. You can easily add Liberty features that are located in the Liberty Repository using either IBM Installation Manager, when installing Liberty, or using the command line, if Liberty is already installed. Both installation methods automatically search for and install any dependencies that the selected features might require.	Show the Installation Manager GUI window where additional features can be installed. Show a command-line window with the featureManager command, displaying options you can use with the command.
9	Additionally, the repository has been integrated with WebSphere Developer Tools and Rational Application Developer so that you can browse, filter, and search assets for these assets. After you find the asset that you want, simply add it to your install cart.	Show the Install Add-ons window in WebSphere Developer Tools. Click <b>Install</b> and hover over the Liberty Repository assets that can be installed.

Table 86. Conclusion. Show where to get started with Liberty Repository

Scene	Audio	Onscreen Action
10	To learn more about the Liberty Repository and the newly added features and assets, go to WASdev.net. Ready to get started?	Show words <i>WASdev</i> and <i>https://www.ibmmdw.net/wasdev/</i> .

For more information, see “Liberty: Liberty Repository” on page 965.

## Video: Why Liberty? Performance that scales

8.5.5.6

The following transcript is for the “Why Liberty? Performance that scales” video, which describes how Liberty delivers optimal performance that easily scales. WebSphere Application Server Liberty is a lightweight, composable application server that is quick to start, easy to manage, and fast to deploy to, which enables rapid application development and availability in mobile, cloud, social, analytic, and enterprise production environments. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content that is shown in the video.

### Why Liberty? Performance that scales

Table 87. Why Liberty? Performance that scales. Show title and then describe how the lightweight and composable nature of Liberty results in a runtime that delivers high performance and scalability.

Scene	Audio	Onscreen Action
1	Why Liberty? Performance that scales	Show title, <i>Why Liberty? Performance that scales</i> .
2	What if your runtime could help you build killer apps that scale?	Show words: What if your runtime could help you build killer applications that scale?

Table 87. Why Liberty? Performance that scales (continued). Show title and then describe how the lightweight and composable nature of Liberty results in a runtime that delivers high performance and scalability.

Scene	Audio	Onscreen Action
3	<p>WebSphere Application Server Liberty is the runtime for IBM Watson® as well as the hybrid cloud solution that serves every Grand Slam Tennis event around the world.</p> <p>So why do Watson™ and the tennis majors use Liberty? Because Liberty delivers the scalability and performance required to support the unique needs of cognitive and analytic queries. Liberty easily scales to meet the demands of real-time major sporting events and analysis applications that can quickly spike to over 100 million web page views at peak match times.</p> <p>Liberty is a lightweight, yet powerful, and fast runtime that was designed and built to meet the needs of developers. Using Liberty, you can rapidly develop and employ applications into production environments that perform and easily scale, which enables you to more quickly transform your own innovative ideas into reality!</p> <p>What if your runtime could help you build killer applications that scale, like Watson or the hybrid cloud solution for Grand Slam Tennis events? It can!</p>	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Australian Open</li> <li>• French Open</li> <li>• Wimbledon</li> <li>• U.S. Open</li> <li>• Liberty can!</li> </ul> <p>Show graphics of:</p> <ul style="list-style-type: none"> <li>• IBM Watson</li> <li>• Liberty</li> <li>• Resizing square scaling graphic for <i>scalability</i></li> <li>• Lightning graphic for <i>performance</i></li> <li>• Multiple pop-up window graphics that show a tennis ball and racquet for <i>web page views</i></li> <li>• Scale graphic for <i>lightweight</i></li> <li>• Speedometer graphic for <i>3-second startup</i></li> <li>• Developer using Liberty</li> <li>• Arrow pointing at the developer with the word <i>You</i> above it</li> <li>• Thought bubble above developer for <i>innovative ideas</i></li> <li>• Thought bubble transferred to the developer's computer screen for <i>reality</i></li> </ul>
4	<p>Liberty is extremely lightweight. With a small memory footprint and fast application startup time, you can be up and running in a matter of seconds. In fact, Liberty is much lighter than the competition!</p>	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Lightweight <ul style="list-style-type: none"> <li>– &lt; 65 MB footprint</li> <li>– &lt; 3-second start up</li> <li>– 40% lighter than the leading competitor</li> </ul> </li> </ul> <p>Show graphic of scale for <i>lightweight</i></p>
5	<p>The installation of Liberty is composable.</p> <p>For a fast startup time, the Liberty installation provides the essential features. If you need more features to meet your application needs, you can easily and quickly install them from the Liberty Repository.</p>	<p>Show words: Composable</p> <p>Show graphics:</p> <ul style="list-style-type: none"> <li>• Show composable nature of Liberty with a foundation of blocks that is built up with more features, or blocks, added.</li> <li>• Show screen capture of Liberty repository and its assets.</li> </ul>

Table 87. Why Liberty? Performance that scales (continued). Show title and then describe how the lightweight and composable nature of Liberty results in a runtime that delivers high performance and scalability.

Scene	Audio	Onscreen Action
6	Liberty complies with the Java Platform Enterprise Edition (Java EE) 7 specification, for both the full platform and its subset, the Java EE 7 Web Profile. This support enables you to code without restrictions and use the latest Java EE 7 capabilities. You can pick and choose the Java EE 7 standard features that you want to use, or you can get all of the features in a convenience feature.	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Fully Java EE 7 compliant               <ul style="list-style-type: none"> <li>– Full platform</li> <li>– Web Profile</li> <li>– Code without restrictions</li> <li>– Use the latest Java EE 7 capabilities</li> </ul> </li> </ul> <p>Show graphics:</p> <ul style="list-style-type: none"> <li>• Java logo</li> <li>• Rolling list of key supported Java EE 7 programming models.</li> <li>• List of Java EE 7 standard features</li> <li>• List of all Java EE 7 features</li> </ul>
7	Liberty can be deployed wherever, whenever and however. You have the flexibility to run in any environment and you can rapidly deploy to the cloud. This capability enables you to achieve even more performance in a short amount of time.	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Whenever</li> <li>• Wherever</li> <li>• However</li> <li>• Rapidly deploy to cloud               <ul style="list-style-type: none"> <li>– On premises</li> <li>– Hosted</li> </ul> </li> </ul> <p>Show graphics:</p> <ul style="list-style-type: none"> <li>• Liberty graphic</li> <li>• Cloud with IBM Bluemix<sup>®</sup></li> <li>• Growing box for <i>performance</i></li> <li>• Shrinking box for <i>time</i></li> </ul>
8	Finally, with the new auto scaling capabilities, you can rapidly scale the number of instances of the run time.	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Scalable               <ul style="list-style-type: none"> <li>– 5 JVMs to 5,000 in minutes</li> </ul> </li> </ul> <p>Show graphic of square graphs quickly multiplying</p>
9	It's not enough to just build a great application. It needs powerful performance and scalability behind it. With these capabilities, Liberty gives you the performance that excels and scalability to meet user demands with fewer hardware and license requirements.	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Lightweight</li> <li>• Composable</li> <li>• Java EE 7</li> <li>• Cloud ready</li> </ul> <p>Show graphics:</p> <ul style="list-style-type: none"> <li>• Resizing square scaling graphic for <i>scalability</i></li> <li>• Lightning graphic for <i>performance</i></li> <li>• Graph for <i>application</i></li> <li>• Shrinking graphics for <i>hardware and license requirements</i></li> </ul>

Table 87. *Why Liberty? Performance that scales (continued)*. Show title and then describe how the lightweight and composable nature of Liberty results in a runtime that delivers high performance and scalability.

Scene	Audio	Onscreen Action
10	There's no better time than now to get started with Liberty -- and it's easy! To download Liberty, and access a wide variety of features, samples, and other tips about developing and extending your applications, visit WASdev.net.	Show words: <ul style="list-style-type: none"> <li>• Getting started is easy</li> <li>• Download Liberty and get features, samples, development tips from WASdev.net</li> </ul>

## Video: Why Liberty? Fast application development

8.5.5.6

The following transcript is for the “Why Liberty? Fast application development” video, which describes how Liberty is simple to install and configure. WebSphere Application Server Liberty is a lightweight, composable application server that is quick to start, easy to manage, and fast to deploy to, which enables rapid application development and availability in mobile, cloud, social, analytic, and enterprise production environments. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content that is shown in the video.

### Why Liberty? Fast application development

Table 88. *Why Liberty? Fast application development*. Show title and then describe how Liberty is simple to install and configure, and how it integrates with WebSphere Developer Tools.

Scene	Audio	Onscreen Action
1	Why Liberty? Fast application development	Show title, <i>Why Liberty? Fast application development</i> .
2	What if your runtime could help you develop apps faster?	Show words: What if your runtime could help you develop apps faster?
3	<p>Did you know you can gain about 8 weeks of time back per year by using WebSphere Application Server Liberty to develop your WebSphere applications?</p> <p>Liberty is simple to use, yet powerful, and was designed and built to meet the needs of developers. Using Liberty, you can rapidly develop and deploy your applications into production environments, which enables you to more quickly transform your own innovative ideas into reality!</p> <p>What if your runtime could give you back weeks each year? It can!</p>	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Gain 8 weeks by using Liberty</li> <li>• Liberty can!</li> </ul> <p>Show graphics:</p> <ul style="list-style-type: none"> <li>• Calendar showing 8 weeks crossed off and now free</li> <li>• Code graphic for <i>simple</i></li> <li>• Lightning graphic for <i>powerful</i></li> <li>• Developer using Liberty</li> <li>• Arrow pointing at the developer with the word <i>You</i> above it</li> <li>• Thought bubble above developer for <i>innovative ideas</i></li> <li>• Thought bubble transferred to the developer's computer screen for <i>reality</i></li> </ul>

Table 88. Why Liberty? Fast application development (continued). Show title and then describe how Liberty is simple to install and configure, and how it integrates with WebSphere Developer Tools.

Scene	Audio	Onscreen Action
4	<p>Liberty is incredibly easy to use.</p> <p>With a footprint of less than 65 MB and a simple archive installation, Liberty provides a lightweight architecture to manage lightning fast, data-rich applications across any web, mobile, or cloud environment with high performance. After downloading Liberty, you can install and configure Liberty, add an application, and have that application running, all in one minute.</p> <p>Liberty has a simple configuration that you can easily share across your development team, store in version control, and edit in real time.</p> <p>When you upgrade your version of Liberty, you can continue to use existing applications and configurations with no changes. There's no need for migration!</p> <p>There are also zero restarts. After you save configuration changes, you do not need to restart Liberty to see the changes go live.</p>	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Liberty is incredibly easy to use</li> <li>• Lightweight <ul style="list-style-type: none"> <li>– &lt; 65 MB footprint</li> <li>– Archive install</li> </ul> </li> <li>• Simple <ul style="list-style-type: none"> <li>– Simple install</li> <li>– Simple XML-based configuration</li> <li>– Zero migration</li> <li>– Zero restarts</li> </ul> </li> </ul> <p>Show graphics:</p> <ul style="list-style-type: none"> <li>• Cloud with Liberty logo sending thunder bolts to devices</li> <li>• For <i>simple install</i>, show install from .zip file</li> <li>• For <i>simple configuration</i>, show changing the server.xml file configuration from WebSphere Developer Tools</li> </ul>
5	<p>WebSphere Developer Tools make it easy to write and deploy applications in Eclipse. Simply drag your application onto your Liberty server.</p> <p>With the IBM Eclipse Tools for Bluemix, you can also quickly and easily deploy to Bluemix.</p>	<p>Show words: WebSphere Developer Tools</p> <p>Show screen capture of WebSphere Developer Tools and dragging a Liberty feature to install it</p>
7	<p>You can build great applications for mobile, cloud, social, analytic, and enterprise production environments without wasted time. Just imagine what you can do with extra weeks gained back each year!</p>	<ul style="list-style-type: none"> <li>• Show graphic of a happy developer</li> <li>• Show developer on vacation</li> </ul>
8	<p>There's no better time than now to get started with Liberty -- and it's easy! To download Liberty, and access a wide variety of features, samples, and other tips about developing and extending your applications, visit WASdev.net.</p>	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Getting started is easy</li> <li>• Download Liberty and get features, samples, development tips from WASdev.net</li> </ul>

## Video: Why Liberty? Rapid deployment and powerful administration

8.5.5.6

The following transcript is for the “Why Liberty? Rapid deployment and powerful administration” video, which describes how Liberty provides a run time to deploy rapidly and easily manage your systems. WebSphere Application Server Liberty is a lightweight, composable application server that is quick to start, easy to manage, and fast to deploy to, which enables rapid application development and availability in mobile, cloud, social, analytic, and enterprise production environments. This transcript is the video storyboard. Audio describes narration and captions. Onscreen Action describes the content that is shown in the video.

 Why Liberty? Rapid deployment and powerful administration

Table 89. Why Liberty? Rapid deployment and powerful administration. Show title and then describe how Liberty is easy to manage and it integrates with open source frameworks.

Scene	Audio	Onscreen Action
1	Why Liberty? Rapid deployment and powerful administration	Show title, <i>Why Liberty? Rapid deployment and powerful administration.</i>
2	What if your runtime could speed up your application deployment?	Show words: What if your runtime could speed up your application deployment?
3	<p>Did you know that with WebSphere Application Server Liberty, you can deploy a large web application over 75% faster than the leading competitor? Not only does Liberty provide a single runtime that meets all of your Java EE needs, it also gives you rapid deployment and powerful administration capabilities.</p> <p>Liberty is a lightweight, but powerful and fast runtime that was designed and built to meet the needs of developers. Using Liberty, you can rapidly develop and deploy your applications into production environments, which enables you to more quickly transform your own innovative ideas into reality!</p> <p>What if your runtime could speed up your application deployment? It can!</p>	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Rapid deployment</li> <li>• Powerful administration</li> <li>• Liberty can!</li> </ul> <p>Show graphics:</p> <ul style="list-style-type: none"> <li>• Liberty logo</li> <li>• Speedometer graphic for <i>75% faster</i></li> <li>• Java EE logo</li> <li>• Scale graphic for <i>lightweight</i></li> <li>• Speedometer graphic for <i>fast</i></li> <li>• Developer using Liberty</li> <li>• Arrow pointing at the developer with the word <i>You</i> above it</li> <li>• Thought bubble above developer for <i>innovative ideas</i></li> <li>• Thought bubble transferred to the developer's computer screen for <i>reality</i></li> </ul>
4	Liberty is easy to manage. Your servers, applications, and other resources are right at your fingertips. With Admin Center, which is accessible from your smartphone, tablet, or computer, you can manage and monitor servers and applications, deploy server packages, and view bookmarked information.	<p>Show words: Liberty is incredibly easy to manage</p> <p>Show graphics for:</p> <ul style="list-style-type: none"> <li>• Show graphic screen captures of using Admin Center.</li> <li>• Show graphic of mentioned devices</li> </ul>

Table 89. Why Liberty? Rapid deployment and powerful administration (continued). Show title and then describe how Liberty is easy to manage and it integrates with open source frameworks.

Scene	Audio	Onscreen Action
5	Liberty integrates seamlessly with open source software. You can take advantage of Spring, Maven, Arquillian, MongoDB, and Docker, just to name a few. You don't need to reinvent the wheel or your existing applications. By leveraging Liberty's flexibility and integrating Liberty into your current development environment, you can be more productive and save valuable time.	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Liberty integrates seamlessly with open source software</li> <li>• Open Source Integration</li> <li>• Software: <ul style="list-style-type: none"> <li>– Tapestry</li> <li>– MongoDB</li> <li>– Cassandra</li> <li>– And more!</li> </ul> </li> <li>• Frameworks: <ul style="list-style-type: none"> <li>– Arquillian</li> <li>– Docker</li> <li>– Spring</li> <li>– Chef</li> <li>– Puppet</li> <li>– And more!</li> </ul> </li> </ul> <p>Show graphics:</p> <ul style="list-style-type: none"> <li>• Wheel and existing applications</li> <li>• Check marks appearing under the graphics</li> </ul>
6	Liberty also supports continuous integration and DevOps. Liberty's fast start up time, small footprint, and simple configuration supports the continuous integration of code into frequent builds and automated testing. With simple build tools for packing the runtime into a single archive, Liberty is easy to deploy in production environments. Additionally, you can use the Liberty Chef cookbooks, which support the use of the Chef DevOps framework.	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Liberty supports continuous integration and DevOps</li> <li>• Simple packaging tools</li> </ul> <p>Show graphics:</p> <ul style="list-style-type: none"> <li>• Apps and codes on a conveyer belt</li> <li>• Check marks above the apps and codes</li> <li>• Screen capture of packaging tools being used</li> <li>• Liberty Chef cookbook on Git</li> </ul>
7	It's not enough to just build a great application, you need to be able to deploy rapidly and easily manage your systems.	<p>Show words:</p> <ul style="list-style-type: none"> <li>• It's not enough to just build a great application</li> <li>• Rapidly deployment</li> <li>• Powerful administration</li> </ul>
8	There's no better time than now to get started with Liberty -- and it's easy! To download Liberty, and access a wide variety of features, samples, and other tips about developing and extending your applications, visit WASdev.net.	<p>Show words:</p> <ul style="list-style-type: none"> <li>• Getting started is easy</li> <li>• Download Liberty and get features, samples, development tips from WASdev.net</li> </ul>

## Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information about the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
1623-14, Shimotsuruma, Yamato-shi  
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
Mail Station P300  
2455 South Road

Poughkeepsie, NY 12601-5400  
USA  
Attention: Information Requests

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. \_enter the year or years\_. All rights reserved.

APACHE INFORMATION. The information center includes all or portions of information which IBM obtained under the terms and conditions of the Apache License Version 2.0, January 2004. The information may also consist of voluntary contributions made by many individuals to the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org>. You may obtain a copy of the Apache License at <http://www.apache.org/licenses/LICENSE-2.0>.

## Programming interface information

This publication primarily documents information that is NOT intended to be used as Programming Interfaces of WebSphere Application Server. This publication also documents intended Programming Interfaces that allow the customer to write programs to obtain the services of WebSphere Application Server. This information is identified where it occurs, either by an introductory statement to a chapter or section or by the following marking: Programming Interface information.

## Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

---

## Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's privacy policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details/us/en> sections entitled "Cookies, Web Beacons and Other Technologies" and "Software Products and Software-as-a Service".



---

## Chapter 2. End-to-end paths for Liberty

### 8.5.5.0

Start here for a step-by-step guidance in working with the WebSphere Application Server Liberty. Identify the scenario that most closely matches with your own project goal, then follow one of the paths through the scenario to achieve your goal.

#### Procedure

- “Enabling JMS messaging for Liberty”
  - “Enabling JMS messaging for a single Liberty server” on page 1122
  - “Enabling JMS messaging between two Liberty servers” on page 1124
  - “Enabling secure JMS messaging for Liberty” on page 1126
  - “Enabling interoperability between Liberty and WebSphere Application Server traditional” on page 1130
  - “Securing JMS communications in Liberty by using SSL” on page 1133
- “Setting up the server-management environment for Liberty by using collectives” on page 1134
  - “Configuring a Liberty collective” on page 1136
  - “Registering host computers with a Liberty collective” on page 1142
  - Overriding server host information
  - “Setting the default host name of a Liberty server” on page 1439
  - “Setting the JAVA\_HOME variable for Liberty collective members” on page 1147
  - “Configuring Liberty collective replica sets” on page 1148
  - Setting up Liberty server clusters
- Setting up Liberty server clusters
  - “Configuring a Liberty server cluster” on page 1155
  - “Starting and stopping a Liberty server cluster” on page 1488
  - “Listing Liberty server clusters and cluster members” on page 1488
  - “Generating a Liberty server cluster plug-in configuration” on page 1489
  - “Managing a Liberty server cluster configuration” on page 1489

---

### Enabling JMS messaging for Liberty



#### 8.5.5.6

Using the `wasJmsServer-1.0` and `wasJmsClient-2.0` Liberty features, you can enable the Java Message Service (JMS) on a single server. To use the `wasJmsServer-1.0` feature in a secure mode, you must enable the `wasJmsSecurity-1.0` feature.

#### Before you begin

The `wasJmsClient-2.0` feature supports the features of both JMS 1.1 and JMS 2.0 specifications. However, you can choose to use the `wasJmsClient-1.1` feature if you want to use only the features that are compliant with JMS 1.1 specification.

## Enabling JMS messaging for a single Liberty server



8.5.5.6

In a development environment, if you want to run the JMS application and JMS messaging run time components on the same server, you can configure the `wasJmsServer-1.0` and `wasJmsClient-2.0` features on the same server. In this scenario, the application is deployed on the same server where the messaging engine and the JMS resources exist. When the application and the messaging engine are deployed on the same server, the application can connect to the messaging engine either over TCP/IP or in-memory API function calls. You can also configure the `wasJmsSecurity-1.0` feature to enable secure connection of the application to the messaging engine.

### Before you begin

The `wasJmsClient-2.0` feature supports the features of both JMS 1.1 and JMS 2.0 specifications. However, you can choose to use the `wasJmsClient-1.1` feature if you want to use only the features that are compliant with JMS 1.1 specification.

## Configuring point-to-point messaging for a single Liberty server



8.5.5.6

You can configure point-to-point messaging such as sending of messages to a queue or receiving of messages from a queue.

### Procedure

1. Configure the messaging features in the `server.xml` file. If you want to perform a JNDI lookup, then you must also add the `jndi-1.0` feature.

```
<featureManager>
  <feature>wasJmsServer-1.0</feature>
  <feature>wasJmsClient-2.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>
```

2. Configure the messaging engine to create a queue, called *libertyQ*, as given in the following example.

```
<messagingEngine>
  <queue id="libertyQ"
    forceReliability="ReliablePersistent"
    maxMessageDepth="5000">
  </queue>
</messagingEngine>
```

3. Declare a queue connection factory resource to create a connection to the messaging engine as given in the following example.

```
<jmsQueueConnectionFactory jndiName="jms/libertyQCF" connectionManagerRef="ConMgr2">
  <properties.wasJms
    nonPersistentMapping="ExpressNonPersistent"
    persistentMapping="ReliablePersistent"/>
</jmsQueueConnectionFactory>
<connectionManager id="ConMgr2" maxPoolSize="2"/>
```

4. Declare a queue resource to create a Producer/Consumer session to the queue, *libertyQ*, as given in the following example.

```
<jmsQueue jndiName="jms/libertyQue">
  <properties.wasJms queueName="libertyQ"
    deliveryMode="Application"
    timeToLive="500000"
    priority="1"
    readAhead="AsConnection" />
</jmsQueue>
```

5. Declare an activation specification for the message-driven beans that are deployed on Liberty. The message-driven beans use the activation specification to asynchronously consume messages from the `jmsQueue` resource.

```
<jmsActivationSpec id="JMSSample/JMSApp/SampleMDB">
  <properties.wasJms destinationRef="jms/libertyQue" />
</jmsActivationSpec>
```

The ID value must be given in the following format: application name/module name/bean name format, where *application name* is the name of the application that is deployed, *module name* is the name of the module in which the bean is packaged, and *bean name* is the *ejb-name* of the enterprise bean. Ensure that the `destinationRef` attribute is pointing to a valid `jmsQueue` resource ID.

**Note:** The application name is applicable only if the bean is packaged within an EAR file.

6. Optional: You can configure the `wasJmsSecurity-1.0` feature to enable the `wasJmsServer-1.0` feature work in a secure mode. For more information, see “Enabling secure JMS messaging for Liberty” on page 1126. The point-to-point messaging is configured to send messages to a queue or to receive messages from a queue.

## Configuring publish and subscribe messaging for a single Liberty server



8.5.5.6

You can configure publish/subscribe messaging from a topic space on a single Liberty server.

### Procedure

1. Configure the messaging features in the `server.xml` file. If you want to perform a JNDI lookup, then you must also add the `jndi-1.0` feature.

```
<featureManager>
  <feature>wasJmsServer-1.0</feature>
  <feature>wasJmsClient-2.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>
```

2. Configure the messaging engine to create a topic space, called *SPORTS*, as given in the following example.

```
<messagingEngine>
  <topicSpace id="SPORTS"
    forceReliability="ReliablePersistent"
    maintainStrictOrder="true"
    maxMessageDepth="5000">
  </topicSpace>
</messagingEngine>
```

3. Declare a topic connection factory resource to create a connection to the messaging engine as given in the following example.

```
<jmsTopicConnectionFactory jndiName="jms/libertyTCF" connectionManagerRef="ConMgr1">
  <properties.wasJms
    clientID="clientId"
    nonPersistentMapping="ExpressNonPersistent"
    password="password"
    persistentMapping="ReliablePersistent"/>
</jmsTopicConnectionFactory>
<connectionManager id="ConMgr1" maxPoolSize="2"/>
```

4. Declare a topic space resource to create a Publisher/Subscriber session to the TopicSpace, *SPORTS*.

```
<jmsTopic jndiName="jms/libertyTopic">
  <properties.wasJms topicName="Cricket"
    deliveryMode="Application"
    timeToLive="500000"
    priority="1"
    readAhead="AsConnection" />
</jmsTopic>
```

5. Declare an activation specification for the message-driven beans that are deployed on Liberty. The message-driven beans use the activation specification to asynchronously consume messages that are published to the `.jmsTopic` resource.

```
<jmsActivationSpec id="JMSSample/JMSApp/SampleMDB">
  <properties.wasJms destinationRef="jms/libertyTopic" />
</jmsActivationSpec>
```

The ID value must be given in the following format: *application name/module name/bean name* format, where *application name* is the name of the application that is deployed, *module name* is the name of the module in which the bean is packaged, and *bean name* is the *ejb-name* of the enterprise bean. Ensure that the `destinationRef` attribute is pointing to a valid `.jmsTopic` resource ID.

**Note:** The application name is applicable only if the bean is packaged within an EAR file.

6. Optional: You can configure the `wasJmsSecurity-1.0` feature to enable the `wasJmsServer-1.0` feature work in a secure mode. For more information, see “Enabling secure JMS messaging for Liberty” on page 1126. The publish/subscribe messaging is configured for a topic queue.

## Enabling JMS messaging between two Liberty servers



8.5.5.6

In a typical production scenario, users might want to run the `wasJmsServer-1.0` and the JMS applications on separate servers to distribute the workload. In such scenarios, you can configure the `wasJmsClient-2.0` Liberty feature on one server, which acts as the client, and configure the `wasJmsServer-1.0` feature on a different server. The JMS applications that are deployed on a remote server always use TCP/IP to connect to the messaging engine that is running on a different server. You can also configure the `wasJmsSecurity-1.0` feature to make your applications to connect securely to the messaging engine, and configure the `ssl-1.0` feature to enable the SSL communication between the two Liberty servers.

### Before you begin

The `wasJmsClient-2.0` feature supports the features of both JMS 1.1 and JMS 2.0 specifications. However, you can choose to use the `wasJmsClient-1.1` feature if you want to use only the features that are compliant with JMS 1.1 specification.

### Configuring the client for enabling JMS messaging between multiple Liberty servers



8.5.5.6

To enable JMS messaging on multiple servers, you must configure the `wasJmsClient-2.0` feature on a different Liberty server.

### Procedure

1. Enable the JMS client feature on the client. If you want to perform a JNDI lookup, then you must also add the `jndi-1.0` feature.

```
<featureManager>
  <feature>wasJmsClient-2.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>
```

2. Configure the required JMS resources.

```
<jmsQueueConnectionFactory jndiName="myQCF" connectionManagerRef="ConMgr4">
  <properties.wasJms
    remoteServerAddress="meserver.ibm.com:7276:BootstrapBasicMessaging" />
</jmsQueueConnectionFactory>
<connectionManager id="ConMgr4" maxPoolSize="2"/>
```

```
<jmsQueue jndiName="myQ">
  <properties.wasJms queueName="libertyQ" />
</jmsQueue>
```

**Note:** To enable the JMS application to perform a remote TCP/IP connection with the remote messaging engine, configure the `<remoteServerAddress>` property of the connection factory. The `<remoteServerAddress>` property refers to the server that has to be contacted, where the messaging engine exists. The property declaration must be as follows:

```
remoteServerAddress="hostname:port:mode"
```

where the *hostname* is the name of the host where the messaging engine is running; *port* is the JMS inbound port that is configured at the server side; and *mode* is *BootstrapBasicMessaging* if SSL is not used, and *BootstrapSecureMessaging* if SSL is used.

If the `<remoteServerAddress>` is not specified, then the JMS application tries to connect to a local messaging engine by default in the same Liberty server.

### 3. Optional: Configure additional properties.

- When the clients are configured to connect remotely to the messaging engine, you can create custom channels, which the application can use to connect to the messaging engine. The two default channels are *BootstrapBasicMessaging* and *BootstrapSecureMessaging*. If you want to override these two channel definitions and use a custom channel, use the `<wasJmsOutbound>` element as follows:

```
<featureManager>
  <feature>wasJmsClient-2.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>
```

```
<wasJmsOutbound id="CustomChain"/>
```

```
<jmsQueueConnectionFactory jndiName="myQCF" connectionManagerRef="ConMgr4">
  <properties.wasJms
    remoteServerAddress="meserver.ibm.com:7276: CustomChain" />
</jmsQueueConnectionFactory>
<connectionManager id="ConMgr4" maxPoolSize="2"/>
```

- When the application uses the *myQCF* connection factory, it uses *CustomChain* to connect to the remote messaging engine instead of using *BootstrapBasicMessaging*. Similarly, if you want to use a secured channel, then you can use the `<useSSL>` option in the `<wasJmsOutbound>` element as given in the following example.

```
<featureManager>
  <feature>wasJmsClient-2.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>
```

```
<wasJmsOutbound id="CustomChainSecured" useSSL="true"/>
```

```
<jmsQueueConnectionFactory jndiName="myQCF" connectionManagerRef="ConMgr4">
  <properties.wasJms
    remoteServerAddress="meserver.ibm.com:7276: CustomChainSecured" />
</jmsQueueConnectionFactory>
<connectionManager id="ConMgr4" maxPoolSize="2"/>
```

The messaging engine is configured to run on the client.

## Configuring the server for enabling JMS messaging between multiple Liberty servers



8.5.5.6

To enable JMS messaging on multiple servers, you must configure the `wasJmsServer-1.0` feature on a different Liberty server.

## Procedure

1. On the Liberty server that is hosting the messaging engine, enable the `wasJmsServer-1.0` feature to initialize the messaging engine to accept the incoming requests.

```
<featureManager>
  <feature>wasJmsServer-1.0</feature>
</featureManager>
```

```
<messagingEngine>
  <queue id="libertyQ"/>
</messagingEngine>
```

2. Optional: Configure additional properties.

The messaging engine listens on port 7276 (unsecured) and 7286 (secured) by default. If you want to bind the messaging engine to a different port, you must use the `<wasJmsEndpoint>` element.

```
<featureManager>
  <feature>wasJmsServer-1.0</feature>
</featureManager>
```

```
<wasJmsEndpoint id="InboundJmsCommsEndpoint" host="*" wasJmsPort="9011" wasJmsSSLPort="9100" />
```

```
<messagingEngine>
  <queue id="libertyQ"/>
</messagingEngine>
```

The `<wasJmsEndpoint>` element defines an inbound JMS communication endpoint, to which the JMS client applications can connect by using the `<wasJmsPort>` element if SSL is not being used, and by using the `<wasJmsSSLPort>` element if SSL is being used. The port number is the one that you specified in the `<remoteAddressServer>` property on the client.

In the previous code example, the messaging engine listens on port 9011 (unsecured) and port 9100 (secured) for accepting the incoming requests.

3. Optional: You can make the `wasJmsServer-1.0` feature work in a secure mode. For more information, see “Enabling secure JMS messaging for Liberty.”
4. Optional: You can secure JMS communications by using SSL. For more information, see “Securing JMS communications in Liberty by using SSL” on page 1133.

For a detailed information about secure communications, see “Securing communications in Liberty” on page 1833. The messaging engine is configured on the Liberty server.

## Enabling secure JMS messaging for Liberty

**8.5.5.0**

Use the `wasJmsSecurity-1.0` Liberty feature to make the `wasJmsServer-1.0` feature work in a secure mode. Securing the messaging resources ensures that only authenticated and authorized users can access the messaging resources such as queues, topics, and messages.

### Authenticating users to connect to the messaging engine

**8.5.5.0**

You must validate the users credentials so that the user is authenticated to connect to the messaging engine.

## Procedure

### 1. Configure the user registry.

The following types of registry are supported in Liberty:

- QuickStartSecurity (supports only one user).

This option is the simplest way of specifying a username and password to authenticate the application connections. You can use the <quickStartSecurity> element to enable a simple (one user) security setup for Liberty. Define the following <quickStartSecurity> element in the server.xml file.

In the following example, the <quickStartSecurity> element is used to define a single user, named *liberty*, with a password of *liberty123*.

```
<quickStartSecurity userName="liberty" userPassword="liberty123"/>
```

**Note:** Ensure that the raw password is not specified (for example, *liberty123*) in the server.xml file. To encode the password, use the security utility tool available with Liberty.

```
<WLP_HOME>\wlp\bin>securityUtility encode "liberty123"
```

For more information about securing passwords, see “Liberty:securityUtility command” on page 1844.

- Basic user registry (supports multiple users and declaration of user groups).

You can configure Liberty to authenticate and authorize users by using the basic user registry. You can set up a basic user registry and configure multiple role mapping in the server.xml file for a Liberty server.

**Note:** The configuration of the <basicRegistry> overrides the <quickStartSecurity> registry.

```
<basicRegistry id="basic" realm="customRealm">
  <user name="user1" password="user1pwd" />
  <user name="user2" password="user2pwd" />
  <user name="user3" password="user3pwd" />
  <user name="user4" password="user4pwd" />
  <user name="user5" password="user5pwd" />
  <user name="user6" password="user6pwd" />
  <user name="user7" password="user7pwd" />
  <user name="user8" password="user8pwd" />
  <group name="Developers">
    <member name="user2" />
    <member name="user4" />
  </group>
  <group name="Testers">
    <member name="user8" />
    <member name="user7" />
  </group>
</basicRegistry>
```

- Lightweight Directory Access Protocol (LDAP) registries (external registries such as Microsoft Active Directory and IBM Directory Server).

You can configure an LDAP server with Liberty for authentication.

```
<ldapRegistry id="LDAP" realm="SampleLdapIDSRealm" host="ctldap1.austin.ibm.com" port="389"
  ignoreCase="true" baseDN="o=ibm,c=us"
  ldapType="IBM Tivoli Directory Server"
  idsFilters="ibm_dir_server"
  searchTimeout="8m">
  <failoverServers name="failoverLdapServers">
    <server host="ralwang.rtp.raleigh.ibm.com" port="389"/>
  </failoverServers>
</ldapRegistry>
```

#### Notes:

- Any user name and password that is specified in the LDAP registry can be specified in the connection factory.

- You can define only one registry type in the `server.xml` file (either a basic registry or an LDAP registry).

For more information about configuring registries, see “Configuring a user registry for Liberty” on page 1851.

## 2. Configuring the application authentication.

Based on the user registry that is specified in the `server.xml` file, you can configure your application in the following ways:

- Specify the user name and password in JMS resources (that is the connection factory and activation specification properties).

The application that uses the connection factory is authenticated against the user name and password specified in the connection factory.

```
<jmsQueueConnectionFactory jndiName="myQCF" connectionManagerRef="ConMgr4">
  <properties.wasJms userName="liberty" password="liberty123"
    remoteServerAddress="localhost:7276:BootstrapBasicMessaging">
  </properties>
</jmsQueueConnectionFactory>
<connectionManager id="ConMgr4" maxPoolSize="2"/>
```

In the previous example, the application that looks for the `myQCF` queue connection factory is automatically authenticated against the user name `liberty` and password `liberty123` that is defined for the configured registry.

- Specifying the user name and password in the JMS application.

**Note:** The user name and password that are specified in the JMS application overrides the user name and password defined in the connection factory.

The application looks up the connection factory property and passes the username and password to authenticate the credentials.

`server.xml`

```
-----
<jmsQueueConnectionFactory jndiName="myQCF" connectionManagerRef="ConMgr4">
  <properties.wasJms
    remoteServerAddress="localhost:7276:BootstrapBasicMessaging">
  </properties>
</jmsQueueConnectionFactory>
<connectionManager id="ConMgr4" maxPoolSize="2"/>
```

Application snippets

```
-----
QueueConnectionFactory qcf = (QueueConnectionFactory) new InitialContext().lookup("myQCF");
QueueConnection qCon = qcf.createQueueConnection("liberty", "liberty123");
```

- Specify the user name and password in the `<containerAuthDataRef>` element.

The default authentication data for the container managed authentication is applicable when bindings do not specify an authentication alias for the resource reference with `res-auth=CONTAINER`. The `<authData>` element must be defined and must be referenced by the service integration bus resources as follows:

```
<authData id="auth1" user="liberty" password="liberty123"/>
```

```
<jmsQueueConnectionFactory jndiName="myQCF"
  containerAuthDataRef="auth1" connectionManagerRef="ConMgr4">
  <properties.wasJms/>
</jmsQueueConnectionFactory>
<connectionManager id="ConMgr4" maxPoolSize="2"/>
```

- Specify the user name and password by using the container managed authentication.

The container managed authentication is applied when bindings specify an authentication alias for a resource reference of `CONTAINER` in the `<res-auth>` element. The following code example shows how the authentication can be specified.

```

server.xml
-----
<authData id="auth1" user="dbuser1" password="{xor}0z0vKDtu"/>

<jmsQueueConnectionFactory id="jndi/myQCF" jndiName="jndi/myQCF" connectionManagerRef="ConMgr4">
  <properties.wasJms/>
</jmsQueueConnectionFactory>
<connectionManager id="ConMgr4" maxPoolSize="2"/>

web.xml
-----
<resource-ref>
  <res-ref-name>jndi/myQCF</res-ref-name>
  <res-auth>Container</res-auth>
  <res-type>javax.jms.QueueConnectionFactory</res-type>
  <lookup-name>jndi/myQCF</lookup-name>
</resource-ref>

ibm-web-bnd.xml (web binding file)
-----
<resource-ref name="jndi/myQCF" binding-name="jndi/myQCF">
  <authentication-alias name="auth1"/>
</resource-ref>

```

After the configuration, the authenticated users need to be assigned the required roles in order to access the messaging resources securely. See “Authorizing users to connect to the messaging engine.”

## Authorizing users to connect to the messaging engine

### 8.5.5.0

You must validate if the authenticated users have sufficient permissions to access the messaging resources (that is queues or topic) to perform actions such as sending, receiving, or browsing messages.

### Procedure

1. Enable the wasJmsSecurity-1.0 feature in the server.xml file.

```

<featureManager>
  <feature>wasJmsServer-1.0</feature>
  <feature>wasJmsClient-2.0</feature>
  <feature>wasJmsSecurity-1.0</feature>
</featureManager>

```

2. Configure the <messagingSecurity> element in the server.xml file to define the role and permission for each user, which will identify the action that they can perform on the messaging resource.

The permissions for the destinations can be defined in the <messagingSecurity> element. The following is a sample configuration:

```

<messagingEngine>
  <queue id="QUEUE1"/>
  <topicSpace id="TopicSpace1"/>

  <messagingSecurity>
    <role name="developer">
      <queuePermission queueRef="QUEUE1">
        <action>SEND</action>
        <action>BROWSE</action>
      </queuePermission>

    <topicPermission topicSpaceRef="TopicSpace1" topicName="Sports/Cricket">
      <action>ALL</action>
    </topicPermission>

    <user name="user1" />
    <user name="user3" />
    <group name="Developers" />

```

```

    </role>

    <role name="tester">
      <queuePermission queueRef="QUEUE1">
        <action>BROWSE</action>
      </queuePermission>

      <topicPermission topicSpaceRef="TopicSpace1">
        <action>RECEIVE</action>
      </topicPermission>

      <user name="user5" />
      <user name="user6" />
      <group name="Testers" />
    </role>
  </messagingSecurity>
</messagingEngine>

```

In the previous configuration, users *user1* and *user3* and the group *Developers* can perform the SEND and BROWSE actions on *QUEUE1*. They can also perform ALL actions on the topics *Sports/Cricket* in *TopicSpace1*. Similarly, users *user5* and *user6* and the group *Testers* can perform the BROWSE action on queue *QUEUE1* and the RECEIVE action on all the topics in *TopicSpace1*.

3. Optional: When you are connecting to the messaging engine, specify the user name and password in the `createConnection` call.

The following is the syntax:

```
[createConnection(userName, password)]
```

Connect to the messaging engine as an authenticated user and perform the operation that is based on the authorization permissions that are declared by the administrator.

## Enabling interoperability between Liberty and WebSphere Application Server traditional

### 8.5.5.0

The JMS applications that are deployed within Liberty can connect to the messaging engine that runs in the WebSphere Application Server traditional (that is, service integration bus). Similarly, the JMS applications that are deployed within the WebSphere Application Server traditional can connect to the messaging engine that runs in Liberty.

### About this task

The following image depicts the interoperability options for configuring your JMS applications to interact between Liberty messaging and service integration bus in WebSphere Application Server traditional.

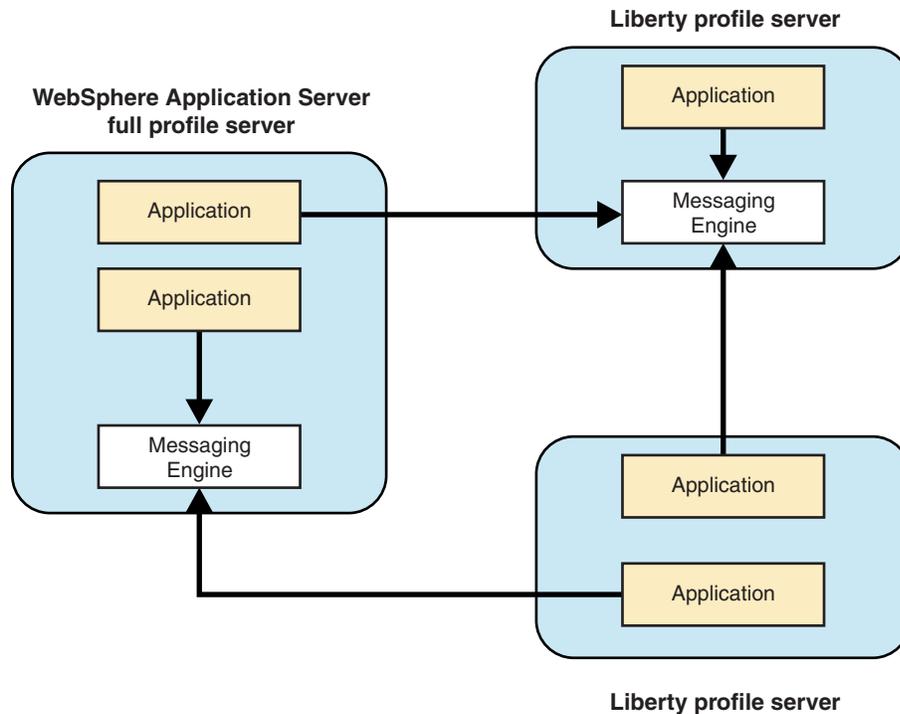


Figure 19. Interoperability between Liberty and WebSphere Application Server traditional

The following tasks provide more information about enabling interoperability between Liberty and WebSphere Application Server traditional.

- “Enabling the JMS application on Liberty to connect to service integration bus”
- “Enabling the JMS application on WebSphere Application Server traditional to connect to Liberty messaging” on page 1132

## Enabling the JMS application on Liberty to connect to service integration bus



8.5.5.6

You can configure the JMS application that is running in Liberty to connect to the service integration bus.

### Procedure

To enable the JMS application to connect to the service integration bus that is running on a WebSphere Application Server traditional server, add the `wasJmsClient-2.0` feature in the `server.xml` file. If you want to perform a JNDI lookup, then you must also add the `jndi-1.0` feature.

```
<featureManager>
  <feature>wasJmsClient-2.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>

<jmsQueueConnectionFactory jndiName="jndi_JMS_BASE_QCF">
  <properties.wasJms
    busName="Bus1"
    remoteServerAddress="localhost:7276:BootStrapBasicMessaging"
    targetTransportChain="InboundBasicMessaging"/>
</jmsQueueConnectionFactory>
```

```
<jmsQueue jndiName="jndi_INPUT_Q">
  <properties.wasJms queueName="Q1" />
</jmsQueue>
```

**Note:** The <remoteServerAddress> must specify the host and port of the server on which the messaging engine is running instead of specifying a bootstrap server.

### Enabling the JMS application on WebSphere Application Server traditional to connect to Liberty messaging:

You can configure JMS applications that are running on the WebSphere Application Server traditional server to connect to Liberty messaging.

#### Procedure

To enable JMS applications that are deployed on the WebSphere Application Server traditional server to connect to Liberty messaging, configure the **Bus name** and the **ProviderEndPoint** in the WebSphere Application Server traditional server to specify the host and port where the Liberty messaging engine is running.

For more information about configuring the bus name in the connection factory in WebSphere Application Server traditional, see Default messaging provider unified connection factory [Settings].

**Note:** The JMS resources that are pointing to the Liberty messaging engine must always specify the **Bus name** as defaultBus (case sensitive).

## Configuring connection pooling for JMS connections

### 8.5.5.1

You can customize the number of concurrent connections (default is 50) that can be created from a JMS connection factory. You can configure connection pooling for a specific JMS connection factory by defining the <connectionManager> element and then associate that element with the JMS connection factory in the server.xml file.

#### Example

The connectionManager element in the server.xml file is used to the connection pool for a JMS connection factory property as given in the following example. The connection pool size is also defined in the connectionManager element.

```
<jmsConnectionFactory id="jmscf1"
  jndiName="jndi/example"
  connectionManagerRef="cm1">
  <properties.wasJms />
</jmsConnectionFactory>
<connectionManager id="cm1" maxPoolSize="10" minPoolSize="2" />
```

The server uses default values for any connection management settings that are not defined on the connectionManager element. If a connection manager is not defined for a connection factory, the server uses the default values for all the settings.

You can define multiple connection factories and associate each with a different connection manager. However, you cannot associate multiple connection factories with a single connection manager.

For more information about the connectionManager element, see .

# Securing JMS communications in Liberty by using SSL

0.5.5.0

You can configure the `ssl-1.0` feature to enable secure communication between the two Liberty servers.

## Before you begin

To secure JMS communications by using SSL, you must configure the SSL feature by providing SSL certificate-related configurations. For more information, see “Enabling SSL communication in Liberty” on page 1834.

## Procedure

### 1. Configure SSL on the server.

- Service integration bus has the following default SSL configuration.

```
<wasJmsEndpoint
  host="*"
  wasJmsSSLPort="7286" >
</wasJmsEndpoint/>
```

Service integration bus inbound uses the `<keyStore>` element as the default SSL configuration. See “Enabling SSL communication in Liberty” on page 1834 for detailed information.

- To modify the configuration to point to a different SSL configuration other than the default, refer to the following example.

```
<keyStore id="customKeyStore" location="key.jks" type="JKS" password="{xor}NDombm1s" />
```

```
<ssl id="CustomSslNewOptions" keyStoreRef="customKeyStore"/>
```

```
<wasJmsEndpoint
  host="*"
  wasJmsSSLPort="7286">
<sslOptions sslRef="CustomSslNewOptions" />
</wasJmsEndpoint>
```

- If the `<wasJmsEndpoint>` configuration is successful, then the service integration bus successfully bounds to port 7286 for secure communications. The JMS client can connect to the messaging engine in a secure way by using SSL.

### 2. Configuring the client

- By default, service integration bus creates an outbound chain that is called `< BootstrapSecureMessaging>`. This chain uses the `<keyStore>` element as a default configuration.

```
<wasJmsOutbound id="BootstrapSecureMessaging"
  useSSL="true">
</wasJmsOutbound>
```

- To change the default SSL configuration to point to some other configuration, refer to the following example:

```
<keyStore id="customKeyStore" location="key.jks" type="JKS" password="{xor}NDombm1s" />
```

```
<ssl id="CustomSslNewOptions" keyStoreRef="customKeyStore"/>
```

```
<wasJmsOutbound id="BootstrapSecureMessaging"
  useSSL="true">
<sslOptions sslRef="CustomSslNewOptions" />
</wasJmsOutbound>
```

- To connect a messaging engine by using the secure communication, specify a secure chain in the `<remoteServerAddress>` element in the connection factory.

```
<jmsQueueConnectionFactory jndiName="jndi_JMS_BASE_QCF">
  <properties.wasJms
    remoteServerAddress="localhost:7286:BootstrapSecureMessaging" />
</jmsQueueConnectionFactory>
```

- You can also create a custom outbound chain and use it to connect to the messaging engine.

```
<keyStore id="customKeyStore" location="key.jks" type="JKS" password="{xor}NDomb1s" />
<ssl id="CustomSslNewOptions" keyStoreRef="customKeyStore"/>

<wasJmsOutbound id="jmsSecureCustomChain"
  useSSL="true">
  <sslOptions sslRef="CustomSslNewOptions" />
</wasJmsOutbound>
```

Now the `<jmsSecureCustomChain>` element is enabled successfully. It uses `<CustomSslNewOptions>` element for SSL keystore configuration.

---

## Setting up the server-management environment for Liberty by using collectives

### 8.5.5.0

To set up the server-management environment for Liberty by using collectives, define the appropriate features in the `server.xml` file and run the corresponding collective command-line tasks to establish the administrative domain security configuration.

### About this task

You can use collectives to manage multiple servers from a single management domain. For high availability, you can configure collective replica sets, clusters, or scaling. For general information about collectives, see “Liberty: Collective architecture” on page 1450.

Liberty provides multiple-server management in the following features:

- **collectiveController-1.0**

The `collectiveController-1.0` feature enables controller functionality for a management collective and includes collective- and cluster-management MBeans that are accessible using the REST JMX connector that is provided by the `restConnector-1.0` feature. The collective controller acts as a storage and collaboration mechanism to which collective members can connect. The administrative domain security configuration for the `collectiveController-1.0` feature is established using the **collective** command-line **create** and **replicate** tasks.

#### Distributed operating systems

IBM i

The `collectiveController-1.0` feature and its capabilities are available only in multiple-server products such as WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in single-server products such as WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a multiple-server product installation, you can use its `collectiveController-1.0` feature to work with collective members from single-server products.

- **collectiveMember-1.0**

The `collectiveMember-1.0` feature enables a server to be a member of a management collective and be managed by the collective controller. The administrative domain security configuration for the `collectiveMember-1.0` feature is established using the **collective** command-line **join** task.

**Tip:** All servers enabled with the `collectiveController-1.0` feature are managed; therefore, you do not need to specify `collectiveMember-1.0` if the server already has the `collectiveController-1.0` feature enabled.

- **clusterMember-1.0**

The cluster member feature enables a collective member to participate in a static cluster.

- **8.5.5.4 dynamicRouting-1.0**

The dynamic routing feature is an Intelligent Management feature of the WebSphere plug-in for Apache and IHS that provides On Demand Router capabilities for the plug-in. The dynamic routing feature enables a server to run a REST service to which the plug-in can connect in order to dynamically route to all servers in a collective.

- **8.5.5.4 scalingController-1.0**

The scaling controller feature enables a collective controller to expand or contract an auto scaling cluster and manage the scaling controller. If an environment has many scaling controllers, only one of the running scaling controllers can make decisions. If that controller is stopped, another running scaling controller takes over for it. The scaling controller can start an auto scaling cluster member in response to increased resource usage, or it might stop an auto scaling cluster member in response to decreased resource usage.

- **8.5.5.4 scalingMember-1.0**

The scaling member feature monitors the workload within a server and its host, then sends this information to the scaling controller. The scaling controller feature is enabled in the collective controllers that are part of the collective. This feature also enables dynamic clustering of the collective members and allows the servers to dynamically start or stop based on criteria that is specified by the scaling policy. If more than one scaling member is on the same host, each scaling member must define a `hostSingleton` element with a port in the `server.xml` file. All scaling members on the same host must use the same port to identify a host leader. The host leader is the only scaling member that communicates with the scaling controller. It communicates metric data from the members to the controller and communicates scaling decisions that are made by the controller to the members in the host.

## Procedure

- Configure a server to act as collective controller.
  - Create a collective controller server using commands and then configure the controller `server.xml` file. See step 1 of “Configuring a Liberty collective” on page 1136.
  - Create a collective controller using developer tools. See step 1 of “Configuring a Liberty collective using the developer tools” on page 1460.
- Join a server to a collective as a member.
  - Join a server to a collective using commands and then configure the member `server.xml` file. See step 2 of “Configuring a Liberty collective” on page 1136.
  - Join a server to a collective using developer tools. See step 2 of “Configuring a Liberty collective using the developer tools” on page 1460.
- Change the collective configuration as needed for your environment.
  - Register host computers with a collective.
  - Override host information by revising parameters in the `hostAuthInfo` element of the member `server.xml` file.
  - Set up Remote Execution and Access (RXA) to enable collective controllers to start and stop servers.
  - Set the `JAVA_HOME` variable for Liberty collective members.
  - Generate collective controller SSL keys.
  - **8.5.5.5** Set administrative metadata for Liberty resources in an `admin-metadata.xml` file.
- Create a replica set, which is a set of collective controllers that are configured to work together, to provide management high availability.
  - **8.5.5.5** Automatically share configurations among replicas.
  - **8.5.5.7** Change the port of a replica.
- Backup, upgrade, or remove a collective controller, replica set, or member.
- Set up static cluster members to provide application high availability and scale.
- **Distributed operating systems** **z/OS** Set up dynamic routing of HTTP requests to collective members.
- **Distributed operating systems** **z/OS** **8.5.5.4** Set up autonomic scaling of collectives.
  - Set up auto scaling for use with Intelligent Management dynamic routing.
  - Configure auto-scalable clusters for JVM elasticity.

- **8.5.5.7** Configure provisionable clusters for Liberty elasticity.
- Define scaling policies.
- **8.5.5.5** Set scaling policies for an auto-scalable cluster in a `scaling-metadata.xml` file.
- **8.5.5.7** Enter maintenance mode before you perform diagnostic tests, maintenance, or tuning on a host or server.
- **8.5.5.7** Configure health management to prevent disruption of service by detecting common problems and generating diagnostic actions based on configured health policies.

## What to do next

You can administer the collective using the following tools:

- Use Jython scripts or a Java client such as JConsole to perform collective controller MBean operations.
- Run collective commands from a command line at the `bin` directory of your Liberty installation. For information about collective commands, run the collective **help** command:

```
wlp/bin/collective help
```

To view details about a specific command, include the command name; for example, to view details about the collective **create** command, run:

```
wlp/bin/collective help create
```

**Tip:** The example commands in this documentation are prefaced with `wlp/bin/`. This means to open a command line at the `bin` directory of your Liberty installation, such as `C:\wlp\bin` on Windows operating systems, and run the command.

- **8.5.5.2** Use WebSphere Liberty Administrative Center ("Admin Center") to administer Liberty servers, applications, and other resources in the collective from a web browser on a smartphone, tablet, or computer.
  1. Add the `adminCenter-1.0` feature to the collective controller `server.xml` file.
  2. To access Admin Center from a smartphone, tablet, or remote computer, ensure that the `server.xml` file sets the `host` attribute of the `httpEndpoint` element to `*` (asterisk) or to a defined host name.
  3. Point a web browser at Admin Center. The URL uses the form:
 

```
https://collective_controller_host_name:collective_controller_port/adminCenter/
```
  4. If your browser prompts you to confirm that the connection is trusted, specify an exception or otherwise enable the connection to continue to Admin Center.
  5. Log in using your collective controller administrative user name and password.
  6. From the Toolbox, open the Server Config tool or Explore tool.
    - **8.5.5.7** Select . Use the Server Config tool to view and edit server configuration files such as `server.xml` files in the collective. For information about the Server Config tool, see "Editing server configuration files in Admin Center" on page 1748.
    - **8.5.5.5** Select . Use the Explore tool to manage applications, clusters, servers, and hosts in the collective. For information about the Explore tool, see "Exploring and managing resources with Admin Center" on page 1749.

For other information about enabling and using Admin Center, see "Administering Liberty using Admin Center" on page 1741.

To ensure that you can remotely start and stop servers, complete the steps for your operating system in "Setting up RXA for Liberty collective operations" on page 1491.

## Configuring a Liberty collective

You can organize Liberty servers into collectives to support clustering, administration, and other operations that act on multiple Liberty servers. By using collectives, you can efficiently and accurately deliver application services to your organization.

## Before you begin

The `collectiveController-1.0` feature and its capabilities are available only in WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a WebSphere Application Server Liberty Network Deployment installation, you can use its `collectiveController-1.0` feature to work with collective members from WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core installations.

## About this task

A Liberty collective is a set of Liberty servers that are configured as part of the same administrative and operational domain.

Configuration and state data about a Liberty collective is housed in an active operational repository.

Membership in a Liberty collective is optional. Liberty servers join a collective by registering with a collective controller to become members. Members share information about themselves through the operational repository of the controller.

The following rules apply:

- A Liberty server can be a member of only one collective.
- Different Liberty servers on the same host can be in different collectives.
- Liberty servers on the same host that are members of a collective can coexist with Liberty servers that are not members of a collective.

 **Watch:** Introduction to creating a collective demonstrates the procedure. This video, and other information about collectives, is available on the WASdev website. [Transcript]

## Procedure

1. Create and configure your controller.
  - a. Create a server to act as the collective controller.

```
wlp/bin/server create myController
```

- b. Create the collective controller configuration.

The collective controller configuration consists primarily of the administrative domain security configuration that is used for secure communication between controllers and members.

```
wlp/bin/collective create myController --keystorePassword=controllerKSPassword
```

**8.5.5.2** By default, this collective command writes all output to a console screen. In the next step, you copy the configuration output into the `server.xml`. To write the configuration to a file instead of to a console screen, specify a `--createConfigFile=outputFilePath` parameter, for example:

```
wlp/bin/collective create myController --keystorePassword=controllerKSPassword --createConfigFile=c:\wlp\usr\servers\myController\
```

After you run the **create** command, the `include` statement to use is displayed. To include the outputted file in the collective configuration, add the `include` statement to the `server.xml` file, for example:

```
<include location="c:\wlp\usr\servers\myController\collective-create-include.xml" />
```

- c. Update the `server.xml` file of the collective controller.

- Copy and paste output.

If the command wrote output to a console screen, proceed with the following steps:

- 1) Copy output from the collective command and paste it into the server.xml file.
- 2) Specify administrative user ID and password values for the collective. For example, change:

```
<quickStartSecurity userName="" userPassword="" />
```

to:

```
<quickStartSecurity userName="adminUser" userPassword="adminPassword" />
```

The default path for the collective controller server.xml file is `${wlp.install.dir}/usr/servers/myController/server.xml` or, if the `$WLP_USER_DIR` variable is set in a server.env file or command window, `$WLP_USER_DIR/servers/myController/server.xml`. After editing, the file will resemble the following example:

```
<server description="controller server">

  <!-- Enable features -->

  <featureManager>
    <feature>jsp-2.2</feature>
  </featureManager>

  <httpEndpoint id="defaultHttpEndpoint"
    host="*"
    httpPort="9080"
    httpsPort="9443" />

  <featureManager>
    <feature>collectiveController-1.0</feature>
  </featureManager>

  <!-- Define the host name for use by the collective.
  If the host name needs to be changed, the server should be
  removed from the collective and re-joined or re-replicated. -->

  <variable name="defaultHostName" value="controllerHostname" />

  <!-- TODO: Set the security configuration for Administrative access -->

  <quickStartSecurity userName="adminUser" userPassword="adminPassword" />

  <!-- clientAuthenticationSupported set to enable bidirectional trust -->

  <ssl id="defaultSSLConfig"
    keyStoreRef="defaultKeyStore"
    trustStoreRef="defaultTrustStore"
    clientAuthenticationSupported="true" />

  <!-- inbound (HTTPS) keystore -->
  <keyStore id="defaultKeyStore" password="yourPassword"
    location="${server.config.dir}/resources/security/key.jks" />

  <!-- inbound (HTTPS) truststore -->
  <keyStore id="defaultTrustStore" password="yourPassword"
    location="${server.config.dir}/resources/security/trust.jks" />

  <!-- server identity keystore -->
  <keyStore id="serverIdentity" password="yourPassword"
    location="${server.config.dir}/resources/collective/serverIdentity.jks" />

  <!-- collective trust keystore -->
  <keyStore id="collectiveTrust" password="yourPassword"
    location="${server.config.dir}/resources/collective/collectiveTrust.jks" />

  <!-- collective root signers keystore -->
  <keyStore id="collectiveRootKeys" password="yourPassword"
    location="${server.config.dir}/resources/collective/rootKeys.jks" />
</server>
```

- **8.5.5.2** Add an include statement.

If you wrote the output to a file by using the `--createConfigFile=outputFilePath` parameter, add an include statement to `$WLP_USER_DIR/servers/myController/server.xml` to include the outputted file in the collective configuration. For example:

```

<server description="controller server">
  <!-- Enable features -->
  <featureManager>
    <feature>jsp-2.2</feature>
  </featureManager>
  <httpEndpoint id="defaultHttpEndpoint"
    host="*"
    httpPort="9080"
    httpsPort="9443" />
  <include location="c:\wlp\usr\servers\myController\collective-create-include.xml" />
</server>

```

Ensure the outputted file sets administrative user ID and password values for the collective, for example:

```
<quickStartSecurity userName="adminUser" userPassword="adminPassword" />
```

- d. Start the collective controller server.

```
wlp/bin/server start myController
```



Figure 20. Collective of one

- e. Verify that the collective controller server started correctly and is ready to receive members.

- 1) Open an editor on the collective controller messages log, \$WLP\_USER\_DIR/servers/myController/logs/messages.log.
- 2) Look for the following message:

```
CWKKX9003I: CollectiveRegistration MBean is available.
```

If you want to enable a collective controller and its members to use the security TLSv1.2 protocol for the Secure Sockets Layer (SSL) context, see “Setting up Liberty to run in SP800-131a” on page 1848. The server.xml files of the controller and members need ssl id elements and each host computer needs a server.env file with the JVM\_ARGS=-Dhttps.protocols=TLSv1.2 statement in its \${wlp.install.dir}/etc directory.

2. Create and configure a member to join the collective.

The controller and members can be on separate hosts. In this example, the controller and member are on the same host.

- a. Create a member server.

```
wlp/bin/server create myMember
```

- b. Join the member.

Run the collective **join** command to join the server to the collective as a member.

The **join** command requires a network connection to the collective controller and an administrative user ID and password for performing MBean operations on the controller. Look at the server.xml file of the collective controller to find the values for the --host, --port, --user, and --password parameters. For --keystorePassword, set a value to use for the member keystore password, such as memberKSPassword. You can specify different --keystorePassword values for each server that is joined to the collective.

```
wlp/bin/collective join myMember --host=controllerHostname --port=9443 --user=adminUser --password=adminPassword --keystorePassword=memberKSPassword
```

The optional parameter --hostname specifies the host name to use for the system. Set --hostname only if the system has multiple host names or does not have its host name configured. If set, the value must match the defaultHostName variable that is defined in the server.xml file.

**8.5.5.2** To write the output of this collective command to a file, instead of to a console screen, specify an optional `--createConfigFile=outputFilePath` parameter. Then, include the outputted file in the collective configuration by adding an `include` statement to the member `server.xml` file:

**8.5.5.2**

```
<include location=outputFilePath />
```

**8.5.5.4** By default, the **join** operation leaves remote procedure call (RPC) credentials undefined. You must specify values for `rpcUser`, `rpcUserPassword`, and the operating system login user and password for the host on which the member server resides. If the member host is registered with the collective controller and the member host is not enabled for SSH, specify an optional `--useHostCredentials` parameter to enable the member to inherit RPC credentials from its host registration on the controller. Typically, Linux hosts are enabled for SSH and Windows hosts are not enabled for SSH; thus, the `--useHostCredentials` parameter is useful for Windows member hosts. Specifying `--useHostCredentials` adds `<hostAuthInfo useHostCredentials="true" />` to the member `server.xml` file. You then can run collective member server commands such as **start** or **stop** without specifying RPC credentials because the member inherits credentials from its host. See “Overriding Liberty server host information” on page 1144 for information about `hostAuthInfo`, the `--useHostCredentials` parameter, and connecting the collective controller to the server.

For information about these required parameters and about optional parameters, run `collective help join` at a command line.

- c. If prompted to accept the certificate chain, enter `y` (yes).
- d. Update the member `server.xml` file.
  - Copy and paste output.

If the command wrote output to a console screen, proceed with the following steps:

- 1) Copy output from the collective command and paste it into the member `server.xml` file.
- 2) Modify the ports so that the server can open its HTTP ports. Ensure the member `server.xml` sets unique HTTP port numbers on its host. For example, if the member is on the same host as the collective controller, change the HTTP port numbers:

```
<httpEndpoint id="defaultHttpEndpoint" httpPort="9081" httpsPort="9444" />
```

Optionally, to access the member server from a remote client, also set `host="*"` in the `httpEndpoint` element.

In `$WLP_USER_DIR/servers/myMember/server.xml`, for example:

```
<server description="member server">
  <!-- Enable features -->

  <featureManager>
    <feature>jsp-2.2</feature>
  </featureManager>

  <httpEndpoint id="defaultHttpEndpoint"
    host="*"
    httpPort="9081"
    httpsPort="9444" />

  <featureManager>
    <feature>collectiveMember-1.0</feature>
  </featureManager>

  <!-- Define the host name for use by the collective.
  If the host name needs to be changed, the server should be
  removed from the collective and re-joined or re-replicated. -->

  <variable name="defaultHostName" value="memberHostname" />
```

**8.5.5.4** `<!-- Remote host authentication configuration --> <hostAuthInfo rpcUser="admin_user_id" rpcUserPassword="admin_user_password" /> <!-- Connection to the`

```

collective controller --> <collectiveMember controllerHost="controllerHostname"
controllerPort="9443" /> <!-- clientAuthenticationSupported set to enable bidirectional trust -->
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore" trustStoreRef="defaultTrustStore"
clientAuthenticationSupported="true" /> <!-- inbound (HTTPS) keystore --> <keyStore
id="defaultKeyStore" password="yourPassword" location="{server.config.dir}/resources/
security/key.jks" /> <!-- inbound (HTTPS) truststore --> <keyStore id="defaultTrustStore"
password="yourPassword" location="{server.config.dir}/resources/security/trust.jks" /> <!--
server identity keystore --> <keyStore id="serverIdentity" password="yourPassword"
location="{server.config.dir}/resources/collective/serverIdentity.jks" /> <!-- collective truststore
--> <keyStore id="collectiveTrust" password="yourPassword" location="{server.config.dir}/
resources/collective/collectiveTrust.jks" /> </server>

```

- **8.5.5.2** Add an include statement.

If you wrote the output to a file by using the `--createConfigFile=outputFilePath` parameter, add an include statement to `$WLP_USER_DIR/servers/myMember/server.xml` to include the outputted file, for example:

```

<server description="member server">
    <!-- Enable features -->

    <featureManager>
        <feature>jsp-2.2</feature>
    </featureManager>

    <httpEndpoint id="defaultHttpEndpoint"
        host="*"
        httpPort="9081"
        httpsPort="9444" />

    <include location="c:\wlp\usr\servers\myMember\collective-join-include.xml" />
</server>

```

- e. **8.5.5.4** If you did not specify `--useHostCredentials` in the `join` command and the member host is not enabled for SSH, set RPC credentials for `hostAuthInfo` in the member `server.xml` file or the outputted file. You can set RPC credentials for the member server in either of two ways:

- Set `hostAuthInfo` RPC user and password values. Set `rpcUser` to an operating system login user ID for the host on which the member server resides, and set `rpcUserPassword` to the operating system login password for the user ID. For example, if you log into the member computer with user `test1` and password `test1pwd`, then change the `hostAuthInfo` element to the following:

```
<hostAuthInfo rpcUser="test1" rpcUserPassword="test1pwd" />
```

- If the member host is registered with the collective controller, set `hostAuthInfo` `useHostCredentials` to `true` for the member server to inherit RPC credentials from its host.

```
<hostAuthInfo useHostCredentials="true" />
```

See “Overriding Liberty server host information” on page 1144 for information about `hostAuthInfo` settings and for an example that shows how to register a member host and run the `join` command with `--useHostCredentials`.

- f. **z/OS** For z/OS only, issue the `updateHost` command to specify the member `JAVA_HOME` directory for the controller.

```

collective updateHost controllerHostname --host=controllerHostname
--port=9443 --user=adminUser --password=adminPassword
--hostWritePath=/dir1 --rpcUser=rpcUser
--rpcUserPassword=rpcUserPassword --hostJavaHome=JAVA_HOME

```

The `hostWritePath` parameter specifies the directories to which the collective controller can write. Paths that are specified by the `hostWritePath` parameter are also readable.

The `hostJavaHome` parameter specifies the absolute path to where the JVM is on the system and where the member server runs, for example `/usr/lpp/java/java_1.7_64`

- g. Start the member server.

```
wlp/bin/server start myMember
```

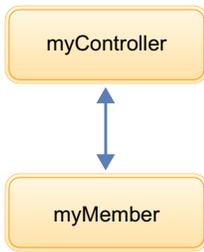


Figure 21. Simple collective

- h. Verify that the member server started correctly and is publishing information to the controller.
  - 1) Open an editor on the member messages log, `$WLP_USER_DIR/servers/myMember/logs/messages.log`.
  - 2) Look for the following messages in any order:
 

```

CWWKX8112I: The server's host information was successfully published to the collective repository.
CWWKX8114I: The server's paths were successfully published to the collective repository.
CWWKX8116I: The server STARTED state was successfully published to the collective repository.
          
```

## Registering host computers with a Liberty collective

### 8.5.5.0

You can register a host computer with a Liberty collective controller, update host information, or unregister a host. Registration enables the collective controller to access applications, command files, and other resources on the host. Registered hosts are members of the collective.

### Before you begin

1. Construct a Liberty collective. See “Configuring a Liberty collective” on page 1136.

#### Distributed operating systems

IBM i

The `collectiveController-1.0` feature and its capabilities are available only in multiple-server products such as WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in single-server products such as WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a multiple-server product installation, you can use its `collectiveController-1.0` feature to work with collective members from single-server products.

2. To enable connections to servers on local and remote hosts, complete the steps for your host operating system in “Setting up RXA for Liberty collective operations” on page 1491. The topic provides information about the Tivoli® Remote Execution and Access (RXA) toolkit and enabling Secure Shell (SSH) protocol. You can use RXA to remotely start and stop servers, including starting and stopping servers on your local computer, and to transfer files to and from registered hosts.

**Note:** **Windows** In Windows, system environment variables are visible only inside the shell that RXA connects to. Setting `PATH` in the command window is not sufficient. You must set `PATH` in the system variable section of the environment variables, or use `-hostJavaHome <PATH TO IBM JAVA>` with the `updateHost` option.

3. If you want to enable a collective controller and its members to use the security TLSv1.2 protocol for the Secure Sockets Layer (SSL) context, see “Setting up Liberty to run in SP800-131a” on page 1848. The `server.xml` files of the controller and members need `ssl id` elements and each host computer needs a `server.env` file with the `JVM_ARGS=-Dhttps.protocols=TLSv1.2` statement in its `${wlp.install.dir}/etc` directory.

## About this task

A host computer is not required to have any WebSphere Application Server products installed. There are no software requirements for a host beyond its operating system. The host can be the same computer on which the product is installed or a different computer.

To register a host with a collective controller, update host information, and unregister a host, use the **registerHost**, **updateHost**, and **unregisterHost** commands. Specify the host computer name in one of the following formats:

- Fully qualified domain name servers (DNS) host name string, such as `xmachine.ibm.com`
- Default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

**Note:** When a Liberty server is joined to a collective, the associated host is automatically registered with the collective controller if it is not already registered.

A host can be registered with the collective under different names. Ensure that the host name specified for **registerHost**, **updateHost**, and **unregisterHost** is consistent with the host name used for the registered collective members. The `defaultHostName` variable in the registered server member's `server.xml` file controls the host name to which the server considers itself to belong.

## Procedure

- Register a host with a collective controller.

To register the current host where both the collective controller host and the remote target host are the same computer, run the **registerHost** command on the collective utility script with no explicit host target. Specify the collective controller's host name, port, and administrative user name and password. For example:

```
wlp/bin/collective registerHost --host=controllerHost --port=controllerHTTPSPort
--user=controllerAdmin --password=controllerAdminPassword
```

This example command generates a unique SSH key pair for authenticating to the SSH server of a specified host computer. If you are registering a remote host for which an SSH key pair is already generated, you can specify the path of the SSH private key file. The following **registerHost** command assumes that the SSH private key is stored on the local controller computer at `/home/user1/.ssh/id_rsa`. The other file in the SSH key pair is the `/home/user1/.ssh/authorized_keys` public key file on the remote target host.

```
wlp/bin/collective registerHost remothost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
--sshPrivateKey=/home/user1/.ssh/id_rsa
```

If the remote target host does not support SSH or you do not want to use SSH keys, you can specify an operating system login user for `rpcUser` and login password for `rpcUserPassword`. If you include `rpcUser` with `rpcUserPassword`, do not include `sshPrivateKey`. The command to specify operating system login user and password resembles:

```
wlp/bin/collective registerHost remothost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
--rpcUser=osUserForRemoteHost --rpcUserPassword=osUserPasswordForRemoteHost
```

### 8.5.5.2

To transfer files to and from a host, you must specify host read and write paths. Unless the **registerHost** command specifies the paths, you cannot deploy a Liberty archive to the host. The `hostReadPath` specifies the directories that the collective controller can read. The `hostWritePath` specifies the directories to which the collective controller can write. Paths that are specified by `hostWritePath` are also readable. For example, to upload an archive to `/opt/wlp`, you must specify `--hostWritePath=/opt`. Specify a parameter multiple times for multiple paths.

```
wlp/bin/collective registerHost myHost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
--rpcUser=osUser --rpcUserPassword=osUserPassword
--hostReadPath=/opt --hostWritePath=/dir1 --hostWritePath=/dir2
```

To use the Deploy tool of the WebSphere Liberty Administrative Center ("Admin Center"), you must set `hostWritePath` to the path to which you want to deploy a server package. To transfer files to multiple directories, include multiple instances of the `hostWritePath` parameter in the command. For example:

```
wlp/bin/collective registerHost myHost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin
--password=controllerAdminPassword --rpcUser=osUser --rpcUserPassword=osUserPassword
--hostWritePath=c:\was\liberty\brokerageAppTest --hostWritePath=c:\wlp_backup
```

**Windows** Before you deploy a server package by using the Deploy tool of Admin Center, complete the steps for your host operating system in "Setting up RXA for Liberty collective operations" on page 1491.

Optionally, specify the path to the Java home directory of the host with the `-hostJavaHome` parameter. For example: `-hostJavaHome=c:\java\jre`

- Update registered host authentication information.

Run the `updateHost` command on the collective utility script to change the authentication information of a registered host. For example, if the user password changes, the following command updates the host password that is used by the collective:

```
wlp/bin/collective updateHost myHost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
--rpcUser=osUser --rpcUserPassword=newOsUserPassword
```

- **8.5.5.2** Update registered host read or write paths.

Run the `updateHost` command on the collective utility script to change the host read and write paths. Paths in this command override the previously set paths for `hostReadPath` and `hostWritePath`, and do not add to the existing paths.

```
wlp/bin/collective updateHost myHost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
--rpcUser=osUser --rpcUserPassword=osUserPassword
--hostReadPath=/optNew --hostWritePath=/opt --hostWritePath=/home/osUser
```

- Unregister a host from a collective controller.

Run the `unregisterHost` command on the collective utility script; for example:

```
wlp/bin/collective unregisterHost myHost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
```

Unregistering a host removes all the registered servers on that host and any other host-based information from the collective controller.

## What to do next

For information about all parameters of the `registerHost`, `updateHost`, and `unregisterHost` commands, see the API documentation for the `CollectiveRegistration` MBean.

## Overriding Liberty server host information

### 8.5.5.0

The `collectiveMember-1.0` feature enables a server to be managed by the collective controller. Most server host information can be automatically detected. In certain scenarios, however, you must provide additional host information so that the collective controller can establish a connection to the server.

**Note:** **Distributed operating systems** **IBM i** The `collectiveController-1.0` feature and its capabilities are available only in WebSphere Application Server Liberty Network Deployment and WebSphere

Application Server Liberty for z/OS. **8.5.5.0** The feature is not available in WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a WebSphere Application Server Liberty Network Deployment installation, you can use

its collectiveController-1.0 feature to work with collective members from WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core installations.

To enable the host information override, add the following element to the server.xml file:

```
<hostAuthInfo rpcPort="ssh_port"
  rpcUser="user_ID"
  rpcUserPassword="password"
  rpcUserHome="user_home"
  rpcHost="host_name"
  sudoUser="sudo_user"
  sudoPassword="sudo_user_password"
  sshPublicKeyPath="public_key_path"
  sshPrivateKeyPath="private_key_path"
  sshPrivateKeyPassword="private_key_password"
```

```
8.5.5.4 useHostCredentials="true_or_false"/>
```

### rpcPort

This parameter specifies the port for the RPC mechanism, which is SSH port 22 by default. If your system uses a nonstandard port, set this value accordingly. If this value is not specified, the default value is 22.

### rpcUser

This parameter specifies the user ID that the collective controller will use to connect to the server. If the host does not support SSH or using SSH keys is not desired, you can use this parameter to specify an operating system login user. For example, if you log in to the host with the myID user, then you specify rpcUser="myID". If this value is not specified, the default value is System.getProperty("user.name").

### rpcUserPassword

This parameter specifies the password for the specified user ID. For example, if you log in to the host with the myID user and the myPwd password, then you specify rpcUser="myID" and rpcUserPassword="myPwd". If this value is not specified, the server will either generate an SSH key pair or use the SSH key pair for the connection that is specified using the **privateKeyPath** and **publicKeyPath** parameters. If SSH is not installed on the server (such as on a Windows or OS/400® operating system), the password is required.

### rpcUserHome

This parameter specifies the home directory of the user. If this value is not specified, the default value is System.getProperty("user.home"). If **rpcUser** is specified, you should specify **rpcUserHome**.

### rpcHost

This parameter specifies the host on which the RPC mechanism is configured to listen. If this value is not specified, the default value is the value of the **defaultHostName** variable. If your system uses a host other than the **defaultHostName**, set this value accordingly.

### sudoUser

If this value is specified, it allows the collective controller to run commands as another, or "sudo", user instead of as the user ID used for the connection. This parameter applies only to servers that have an SSH server installed. This parameter has no default value.

### sudoPassword

This parameter specifies the password for the sudo user specified by the **sudoUser** parameter. This parameter applies only to servers that have an SSH server installed. This parameter has no default value.

### sshPublicKeyPath

This parameter specifies the path and file name of a user-specified public key file. If this value is not

specified, the default is `${server.output.dir}/resources/security/ssh/id_rsa.pub`. If the specified file (or default file) does not exist, a new public key file will be generated.

### **sshPrivateKeyPath**

This parameter specifies the path and file name of a user-specified private key file. If this value is not specified, the default is `${server.output.dir}/resources/security/ssh/id_rsa`. If the specified file (or default file) does not exist, a new private key file will be generated.

### **sshPrivateKeyPassword**

This parameter specifies the password for the private key. This parameter has no default value.

#### **8.5.5.4 useHostCredentials**

This parameter specifies whether collective member server commands inherit RPC credentials from the host. The default is `false`, requiring the user to specify RPC credentials for the controller to remotely start or stop the member. When set to `true`, collective member server commands inherit RPC credentials from the host registration and ignore all other RPC credentials in the `hostAuthInfo` configuration element.

## **Examples**

Scenario 1: Server is on Windows operating system, no SSH is installed

```
<hostAuthInfo rpcUserPassword="myPassword"/>
```

Scenario 2: Server has SSH installed, SSH is running on port 2222

```
<hostAuthInfo rpcPort="2222"/>
```

Scenario 3: Need to run commands as another user

```
<hostAuthInfo sudoUser="anotherUser" sudoPassword="anotherPassword"/>
```

Scenario 4: Server is on a Windows operating system and `ssh` (e.g. `Cygwin`) is installed. With the following server configuration, the controller connects the member server with `ssh`. In this case, the requirement to disable Windows User Account Control (UAC) does not apply. The parameter `<user's home directory>` is the user default home directory, for example: `C:\cygwin\home\bob`

```
<hostAuthInfo rpcUserHome="<user's home directory">"/>
```

**8.5.5.4** Scenario 5: The collective controller and member are on separate hosts, and not on the same host. To specify that the member inherit RPC credentials from the host, set `useHostCredentials` to `true` in the `server.xml` file of the member. Complete the following steps to configure the member to inherit RPC credentials from the host by specifying `--useHostCredentials` in the `join` command that joins a server as a member to the collective.

1. Create, configure, and start a collective controller named `myController` as shown in step 1 of “Configuring a Liberty collective” on page 1136.
2. Register the host for the member with the collective. The member and the collective controller are on different hosts.

In this scenario, the `registerHost` command uses the collective controller host `hostA.ibm.com` with port number 9443, user `admin`, and password `adminpwd`. The command registers the member host `hostB.ibm.com` with the collective, and sets `rpcUser` to an operating system login user ID for the member host `osUser1`, and `rpcUserPassword` to the operating system login password for the user ID for the member host `osUser1Pwd`. Run the `registerHost` command on the collective controller host.

```
wlp/bin/collective registerHost hostB.ibm.com --host=hostA.ibm.com --port=9443 --user=admin --password=adminpwd --rpcUser=osUser1 --
```

Enter `y` (yes) when prompted to accept the certificate chain. After registration, the Host `hostB.ibm.com` successfully registered. message displays. The collective controller host now has the operating system user ID and password of the member host.

3. On the member host, create a server named `myMember` to use as a collective member.

```
wlp/bin/server create myMember
```

4. Add the myMember server to the collective controller, specifying to use host credentials. In the **join** command, which is run on the member host, specify `--useHostCredentials` so that the member inherits RPC credentials from the host registration.

```
wlp/bin/collective join myMember --host=hostA.ibm.com --port=9443 --user=admin --password=adminpwd --keystorePassword=memberKSPas
```

5. Update the member server.xml file as shown in step 2 of “Configuring a Liberty collective” on page 1136.

Because you specified `--useHostCredentials` in the **join** command, the configuration generated for the member server.xml file sets `useHostCredentials` to `true`:

```
<!-- Remote host authentication configuration -->  
<hostAuthInfo useHostCredentials="true" />
```

With the `--useHostCredentials` option, you do not need to specify the operating system user ID and password in the member server.xml file because the member inherits credentials from the host. Later, if the operating system user ID or password of the member server changes, run the **updateHost** command to change the user ID or password. For more information about the **registerHost** and **updateHost** commands, see “Registering host computers with a Liberty collective” on page 1142.

## Setting the JAVA\_HOME variable for Liberty collective members

All Liberty collective members must have a Java Runtime Environment (JRE) installed that meets the minimum requirements of the Liberty server. After a JRE is installed on the host computer, you can set the `JAVA_HOME` variable so that the Liberty operation can locate the JRE.

### About this task

In order for the collective controller to perform remote operations on Windows members such as starting or stopping a member server, the collective controller must run with an IBM JRE. Third-party JREs do not contain the required security classes. You can get a JRE that supports Liberty products and SSL from Installation Manager offerings or developerWorks:

- Using Installation Manager, select the Liberty product first and then select WebSphere SDK for Liberty. Use Installation Manager to install the Liberty product and software development kit (SDK). The WebSphere SDK for Liberty includes the needed support for Liberty products and SSL and offers a Java client, JConsole.
- Go to <http://www.ibm.com/developerworks/java/jdk/index.html> on the developerWorks website and download an IBM Java development kit (JDK) for your operating system. The developerWorks website does not have a JRE for all operating systems. For example, you have to get the JDK from Eclipse for Windows operating systems.

You can set the `JAVA_HOME` variable in operating system settings or at a command line. Setting set the `JAVA_HOME` variable enables remote operations to locate the JRE.

### Procedure

- **Windows** To set `JAVA_HOME` on a Windows system, perform the following actions.

1. On the Control Panel, do the following:
  - Click **System**.
  - Click **Advanced system settings**.

The System Properties window opens.

2. Click the **Environment Variables** button.
3. Click the *New* button in the system-variables section.
4. Add the `JAVA_HOME` variable name and specify a path to the jre directory; for example:  
`C:\wlp_855\IBM\WebSphere\Liberty\java\java_1.7.1_64\jre`

Some collective controller commands require that the path to the Java installation `jre\bin` directory be available in the System path, so also add a path to the `jre\bin` directory.

5. Save the changes. You might need to reboot the computer for the changes to take effect.
6. To verify the changes, at a command line enter `set JAVA_HOME`. The command displays the `JAVA_HOME` settings; for example:

```
JAVA_HOME=C:\wlp_855\IBM\WebSphere\Liberty\java\java_1.7.1_64\jre
```

**Note:** Rather than change operating system settings, you can set `JAVA_HOME` at a command line by entering `set JAVA_HOME=path_to_jre`. A limitation is that the `JAVA_HOME` setting only applies to commands entered in the same command window.

- **AIX** **HP-UX** **Linux** **Solaris** If you are running bash shell, you can add the `JAVA_HOME` environment variable to the `.bashrc` file in the user's home directory.
- One option for setting `JAVA_HOME` is to create a `server.env` file in the `${server.config.dir}` where `server.xml` is residing and add `JAVA_HOME` there.

For example:

```
JAVA_HOME=/java/jre
```

**Linux** Some collective controller commands require that the path to the Java installation `jre/bin` directory be available in the `.bashrc` file, so set a path to `jre/bin` in the `.bashrc` file.

## Configuring Liberty collective replica sets

You can configure collective replica sets. A replica set provides highly available management capabilities for a Liberty administrative domain.

**Distributed operating systems**

**IBM i**

### Before you begin

The `collectiveController-1.0` feature and its capabilities are available only in WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a WebSphere Application Server Liberty Network Deployment installation, you can use its `collectiveController-1.0` feature to work with collective members from WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core installations. A collective member can be from any WebSphere Application Server Liberty release.

### About this task

A *replica set* is a set of collective controllers that are configured to work together. Each replica contains all the repository updates that the other replicas within the set have processed. Therefore, there is no need for a member or client to connect with a particular collective controller each time that it interacts with the collective; any of the collective controllers that are configured in the replica set can provide the same data.

For detailed instructions about creating and configuring a collective controller, see “Configuring a Liberty collective” on page 1136.

You can complete the following procedures to configure a collective replica set:

1. Add a replica to an existing replica set.
2. Modify the default configuration of the initial replica set.

See Example: Create and activate a replica set for an example of creating a replica set consisting of three collective controllers on the same host.

### Procedure

1. Add a replica to an existing replica set.

During the life of a replica set, it might become necessary to add one or more replicas to an existing set, to increase capacity for example.

The existing replicas in the replica set do not require any updates to their configuration. You can update them so that their configurations in the `server.xml` files more accurately reflect the replicas that form the replica set, but this update is unnecessary and does not affect their behaviors.

**Note:** It is not necessary to change the `replicaSet` value in the `server.xml` file of an existing replica in the set. No change to the configuration of an existing replica is required. If you do want to update the `replicaSet` values in the configurations of existing replicas in the set so that the configuration values are consistent across all replicas in the set, you must set the `isInitialReplicaSet` value in the configurations of the existing replicas to `false`. After you alter the `replicaSet` value, it describes a changed replica set rather than the initial replica set.

**Note:** When you refer to a replica, you must be consistent and use the same `host:port` value. If a hostname is used, it must always be used. Or, if an IP address is used, it must always be used.

To add a replica, follow these steps:

- a. Ensure that the existing replica set is running and that most of the replicas are available.
- b. Create a server to be the new collective controller.

```
wlp/bin/server create MyNewController
```

- c. Replicate to transform the new server into a collective controller.

```
wlp/bin/collective replicate MyNewController
--host=host_of_running_controller
--port=https_port_of_running_controller
--user=username_for_running_controller
--password=userPassword_for_running_controller
--keystorePassword=keystore_password_for_new_controller
```

The `replicate` command writes XML output to a console screen. You copy the output into the `server.xml` file.

**8.5.5.2** To write the output of the command to a file, instead of to a console screen, specify the `--createConfigFile=output_file_path` parameter. Then, include the outputted file in the collective configuration by adding an `include` statement to the `server.xml` file:

```
<include location=output_file_path />
```

- d. Configure the new replica's `server.xml` file by using output of the `replicate` command.

Copy the XML output of the `replicate` command into the `server.xml` file. You can modify the replica configuration as follows:

- **Required settings:**

The values must be explicitly set. The XML printed by the `replicate` command contains this configuration and is sufficient for these settings.

**8.5.5.4 hostAuthInfo**

Host authentication information containing properties that a remote client needs to start the server. This setting is only required when the host of the new replica is not enabled for SSH. Typically, Linux hosts are enabled for SSH and Windows hosts are not enabled for SSH. Thus, this setting might only be needed on Windows hosts. Set RPC credentials for the replica in either of two ways:

- Set `rpcUser` to an operating system login user ID for the host on which the replica resides, and set `rpcUserPassword` to the operating system login password for the user ID. For example, if you log into the replica computer with user `test1` and password `test1pwd`, then change the `hostAuthInfo` element to the following:

```
<hostAuthInfo rpcUser="test1" rpcUserPassword="test1pwd" />
```

- If the replica host is registered with the collective controller, set `hostAuthInfo useHostCredentials` to `true` for the replica to inherit RPC credentials from its host.

```
<hostAuthInfo useHostCredentials="true" />
```

See “Overriding Liberty server host information” on page 1144 for information about `hostAuthInfo` settings.

### **replicaSet**

Space-delimited list that contains the `host:port` for each of the `replicaHosts` and `replicaPorts` in the replica set, excluding the values for the collective controller now being added to the set

For example,

```
original.host.com:10001 some.other.host.com:10003
```

At least one of the values in this set must already be a replica of the existing replica set.

- **Optional settings:**

These settings default, but can be altered.

### **isInitialReplicaSet**

False

### **replicaHost**

Hostname for each individual replica

### **replicaPort**

Port for each individual replica

This port is not the `http` or `https` port of the collective controller, but it is a unique port that is used for communication between the replicas of the replica set.

### **repositoryDir**

Directory location that is used to store repository data

Here is an example of what you might add to a new replica `server.xml` file:

```
<collectiveController replicaHost="localhost"
  replicaPort="10012"
  replicaSet="localhost:10010 localhost:10011"
  isInitialReplicaSet="false"/>
```

The XML printed by the **replicate** command requires updating the server's security configuration and specifying the `collectiveRootKeys` keystore password. The server's security configuration should be identical to the original collective controller's configuration, and the `collectiveRootKeys` keystore password should be the password that is used for the original collective controller's `collectiveRootKeys` keystore password. If the replica was created from the controller that is created in “Configuring a Liberty collective” on page 1136, the new controller's configuration should contain the following:

```
<quickStartSecurity userName="adminUser" userPassword="adminPassword" />
<!-- collective root signers keystore -->
<keyStore id="collectiveRootKeys" password="yourPassword"
  location="{server.config.dir}/resources/collective/rootKeys.jks" />
```

- e. Start the new replica by starting the new collective controller.
- f. Confirm that the original collective controller successfully connected to the new replica. Look for message `CWWKX6009I` in the `messages.log` file of the original collective controller and the replica.

**Tip:** For scripts that run the **replicate** and **addReplica** commands, add a 10-second wait after the **replicate** command runs to ensure the original collective controller and replica connect before running the **addReplica** command.

- g. Invoke the `addReplica` operation on the collective utility to activate the new replica. The argument to the `addReplica` set must be the replica endpoint (in the form "`replicaHost:replicaPort`") of the replica to add.

```
wlp/bin/collective addReplica localhost:10012
  --host=host_of_running_controller
  --port=port_of_running_controller
  --user=user_for_running_controller
  --password=user_password
```

- Optional: If necessary, you can modify the default configuration of the initial replica set. This step is recommended but not required.

The configuration of the initial replica set occurs when the initial collective controller is created. If it is necessary to modify the default replica configuration, the following properties can be changed in the `server.xml` file:

**Optional settings:** These values default, but can be altered.

**replicaHost**

Hostname for each individual replica

**replicaPort**

Port for each individual replica

This port is not the http or https port of the collective controller, but it is a unique port that is used for communication between the replicas of the replica set.

**repositoryDir**

Directory location that is used to store the repository data

## Example: Creating and activating a replica set

This example describes how to create a replica set and then activate it. A replica set must have at least three replicas, preferably on different hosts, for high availability. This example has the replicas on the same host, which requires that you assign unique port numbers for the replicas. When replicas are on different hosts, the replicas can use the same port numbers.

1. Create a replica set.

To create a replica set, you increase the number of collective controllers and configure them so that they can communicate with each other. Each new collective controller is called a *replica* because the added collective controllers have the same security configuration as the original controller and because all information written to any one controller is automatically replicated to all other active controllers. Once configured, all collective controllers in the replica set can perform the same operations as the original controller.

- a. If you do not have a collective controller, create one. See step 1 of “Configuring a Liberty collective” on page 1136.
- b. Ensure the existing collective controller is running. For an existing controller named `myController`, run the **status** command:

```
wlp/bin/server status myController
```

If the collective controller is not running, then start it using the **start** or **run** command:

```
wlp/bin/server start myController
```

- c. Create a server to be the new collective controller.

```
wlp/bin/server create myController2
```

- d. Replicate the existing collective controller configuration into the new collective controller. The new collective controller is called a *replica*.

Run a **replicate** command that uses the administrative security domain configuration of the existing collective controller and sets a new keystore password for the replica. Look at the `server.xml` file of the existing collective controller to find the values for the `--host`, `--port`, `--user`, and `--password` parameters. For `--keystorePassword`, set a value to use for the keystore, such as `myController2`. For information about these required parameters and about optional parameters, run `collective help replicate` at a command line.

```
wlp/bin/collective replicate myController2 --host=host_of_existing_controller --port=https_port_of_existing_controller --user=user
```

If prompted to accept the certificate chain, enter `y` (yes).

The **replicate** command writes XML output to a console screen. You copy the output into the `server.xml` file.

**8.5.5.2** To write the output of the command to a file, instead of to a console screen, specify the `--createConfigFile=output_file_path` parameter. Then, include the outputted file in the collective configuration by adding an `include` statement to the `server.xml` file:

```
<include location=output_file_path />
```

- e. Add the XML output of the **replicate** command into the `server.xml` file of the replica and edit the parameter values as needed.
- Ensure that the `httpEndpoint` element sets `replica httpPort` and `httpsPort` values that are unique port numbers on the host. For example, suppose the original controller named `myController` and the replica are both on the same localhost and `myController` has the following the `httpEndpoint` element:

```
<httpEndpoint id="defaultHttpEndpoint"
  host="*"
  httpPort="9080"
  httpsPort="9443" />
```

Change the values for `myController2` to:

```
<httpEndpoint id="defaultHttpEndpoint"
  host="*"
  httpPort="9085"
  httpsPort="9448" />
```

- **8.5.5.4** Set RPC credentials for `hostAuthInfo`. You can set RPC credentials for the replica in either of two ways:

- Set `hostAuthInfo` RPC user and password values. Set `rpcUser` to an operating system login user ID for the host on which the replica resides, and set `rpcUserPassword` to the operating system login password for the user ID. For example, if you log into the replica computer with user `test1` and password `test1pwd`, then change the `hostAuthInfo` element to the following:

```
<hostAuthInfo rpcUser="test1" rpcUserPassword="test1pwd" />
```

- If the replica host is registered with the collective controller, set `hostAuthInfo useHostCredentials` to `true` for the replica to inherit RPC credentials from its host.

```
<hostAuthInfo useHostCredentials="true" />
```

See “Overriding Liberty server host information” on page 1144 for information about `hostAuthInfo` settings.

- Ensure that `replicaPort` sets a port number for the replica that is unique among the replica set and that `replicaSet` sets `host:port` values that identify the replica set. For example, if the original controller named `myController` and the replica are both on the same localhost, change the values for `myController2` from `null`:

```
<collectiveController replicaPort="null"
  replicaSet="localhost:null"
  isInitialReplicaSet="false" />
```

to 10011 for the replica port and 10010 for the replica set port:

```
<collectiveController replicaPort="10011"
  replicaSet="localhost:10010"
  isInitialReplicaSet="false" />
```

- Ensure the security configuration sets the same values as those used by the original controller. For example, both `myController` and the `myController2` replica use:

```
<quickStartSecurity userName="adminUser" userPassword="adminPassword" />
```

- Ensure the collective root signers keystore element sets the same password as that used by the original controller. For example, copy the `collectiveRootKeys` keystore password from the `myController` `server.xml` file and paste it into the `myController2` replica `server.xml` file. This example shows a generated password:

```
<!-- collective root signers keystore -->
<keyStore id="collectiveRootKeys" password="{xor}Lz4sLCgwLTs="
  location="{server.config.dir}/resources/collective/rootKeys.jks"/>
```

- f. Start the new replica by starting the new collective controller.

```
wlp/bin/server start myController2
```

g. Verify that the original collective controller can communicate with the new replica.

- 1) Open an editor on the original controller messages log, `$WLP_USER_DIR/servers/myController/logs/messages.log`.
- 2) Look for the following message, which might have different IP addresses in your environment:

```
CWWKX6009I: The collective controller successfully connected to replica 127.0.0.1:10011. Current active replica set is [127.0.0.1:
```

h. Verify that the new replica can communicate with the original collective controller.

- 1) Open an editor on the replica messages log, `$WLP_USER_DIR/servers/myController2/logs/messages.log`.
- 2) Look for the following message, which might have different IP addresses in your environment:

```
CWWKX6009I: The collective controller successfully connected to replica 127.0.0.1:10010. Current active replica set is []. The con
```

2. Activate the new replica.

Run an **addReplica** command that uses the administrative security domain configuration of the collective controller and specifies the endpoint of the replica that you want to activate in the form `replicaHost:replicaPort`. Look at the `server.xml` file of the collective controller to find the values for the `--host`, `--port`, `--user`, and `--password` parameters. Look at the `server.xml` file of the replica to find the values for `replicaHost:replicaPort`. For information about these parameters, run `collective help addReplica` at a command line.

```
wlp/bin/collective addReplica replicaHost:replicaPort --host=host_of_existing_controller --port=port_of_existing_controller --use
```

For this example, which has the existing collective controller and the replica on the same host, `localhost`, run:

```
wlp/bin/collective addReplica localhost:10011 --host=localhost --port=9443 --user=adminUser --password=adminPassword
```

If prompted to accept the certificate chain, enter `y` (yes).

3. Repeat steps 1 and 2 for additional replicas. For example, add a third replica to the replica set. Name the new replica `myController3` and specify `replicaPort="10012"`. A replica set must have at least three replicas for high availability.

After the third replica is added to the replica set, you can verify that the original collective controller and new replicas synchronized successfully.

- Look for the following messages in the original controller messages log. The messages might have different IP addresses in your environment:

```
CWWKX6015I: A request to change the active collective controller replica set was received and is now processing. The current active
```

```
CWWKX6016I: The active collective controller replica set changed successfully. The current active replica set is {127.0.0.1:10010,
```

```
CWWKX6011I: The collective controller is ready, and can accept requests. The leader is 127.0.0.1:10010. Current active replica set
```

```
CWWKX6014I: This collective controller replica finished synchronizing the data with the other replicas.
```

- Look for the following messages in the messages logs of the added replicas. The messages might have different IP addresses in your environment:

```
CWWKX6016I: The active collective controller replica set changed successfully. The current active replica set is {127.0.0.1:10010,
```

```
CWWKX6011I: The collective controller is ready, and can accept requests. The leader is 127.0.0.1:10010. Current active replica set
```

```
CWWKX8112I: The server's host information was successfully published to the collective repository.
```

```
CWWKX8114I: The server's paths were successfully published to the collective repository.
```

```
CWWKX8116I: The server STARTED state was successfully published to the collective repository.
```

## Setting up Liberty server clusters

8.5.5.0

A Liberty can be configured into a server cluster for application high availability and scale.

The `collectiveController-1.0` feature and its capabilities are available only in multiple-server products such as WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in single-server products such as WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a multiple-server product installation, you can use its `collectiveController-1.0` feature to work with collective members from single-server products.

A Liberty server cluster is comprised of two or more Liberty servers configured into a server cluster within a Liberty collective. A Liberty server cluster has a unique name within the collective. The `collectiveController-1.0` feature supports several operations on Liberty server clusters through the `ClusterManager` MBean:

- List clusters
- Start cluster
- Stop cluster
- List cluster members
- Generate cluster plug-in configuration

To be part of a server cluster, a Liberty must be a member of a Liberty collective and also be configured with the `clusterMember` feature.

A collective member can be a member of only one server cluster. All cluster members must be members of the same collective. Multiple server clusters can be configured within the same collective. The following diagram illustrates these relationships.

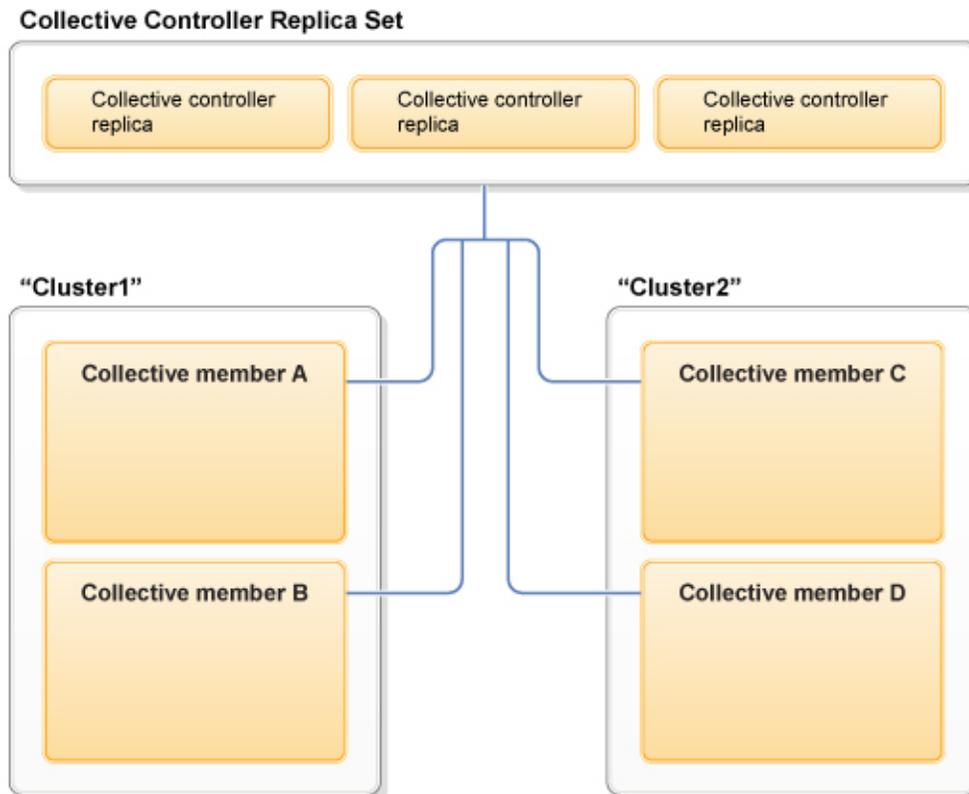


Figure 22. Liberty server clusters

## Configuring a Liberty server cluster

You can configure a collective member to be part of a server cluster by adding the `clusterMember-1.0` feature to the `member server.xml` file. Optionally, you can specify a cluster name to place the member in a particular server cluster. A server cluster has a unique name within a Liberty collective. All Liberty servers that specify the same cluster name within the same collective are members of the same server cluster.

### Before you begin

To be a member of a server cluster, a Liberty server must also be a member of a Liberty collective. If you do not have a Liberty collective and member already, create a collective controller and member server to join the collective. See “Configuring a Liberty collective” on page 1136.

### Procedure

1. Add the `clusterMember-1.0` feature to the feature manager of the `member server.xml` file.

```
<featureManager>
  <feature>collectiveMember-1.0</feature>
  <feature>clusterMember-1.0</feature>
</featureManager>
```

2. Optional: To designate that the member belong to a particular server cluster, add a `clusterMember` element that specifies a cluster name.

For example, place the member in the `myCluster` cluster:

```
<featureManager>
  <feature>collectiveMember-1.0</feature>
  <feature>clusterMember-1.0</feature>
</featureManager>
<clusterMember name="myCluster"/>
```

The default cluster name is `defaultCluster`. If the `member server.xml` does not have a `clusterMember` element that specifies a valid cluster name, then the member is added to `defaultCluster`.

Only specify one cluster name. A single collective can have multiple clusters, but a server can only be part of one cluster at a time.

3. If the collective controller and member server are not running, then start them.

The collective controller and member server must be running for the member to be added to the cluster. For example, use the **start** command to start a collective controller named `myController` and a member named `myMember`:

```
wlp/bin/server start myController

wlp/bin/server start myMember
```

You can configure a collective member to be a cluster member while the member server is running. The new configuration is updated dynamically and published to the collective controller. If you configure a collective member to be a cluster member while the member server is stopped, the member server will not become a member of a cluster until the server starts.

4. Verify that the member is part of the cluster.

- a. Look for a message that indicates the collective member now belongs to the cluster in the collective controller messages log.

The default path for the log is `${wlp.install.dir}/usr/servers/myController/logs/messages.log` or, if the `$WLP_USER_DIR` variable is set in a `server.env` file or command window, `$WLP_USER_DIR/servers/myController/logs/messages.log`.

```
CWWKX9051I: The myMember server has been added to the myCluster cluster.
```

- b. Look for messages that indicate the collective member is now a cluster member in the member messages log, `$WLP_USER_DIR/servers/myMember/logs/messages.log`.

```
CWWKX7400I: The ClusterMember MBean is available.
           myCluster
```

```
CWWKF0012I: The server installed the following features: [clusterMember-1.0].
```

## What to do next

To enable application security for the cluster, copy the LTPA key file from one of the cluster members to all the other members in the cluster. See “Creating a Liberty cluster with security considerations” on page 1488.

To administer the cluster, you can run collective controller `ClusterManager` MBean operations such as start or stop the server cluster, list clusters and cluster members in the collective, or generate a plug-in configuration file. You can run the operations using Jython scripts or a Java client such as JConsole.

**8.5.5.4** Also, you can use WebSphere Liberty Administrative Center (“Admin Center”) to administer the cluster and its servers, applications, and other resources from a web browser. See “Administering Liberty using Admin Center” on page 1741.

**8.5.5.4** After configuring a *static cluster*, which this topic describes, you can route application requests to Liberty servers using IBM HTTP Server (IHS). Static clusters can receive requests through either static or dynamic routing. For information about static routing, see “Generating a Liberty server cluster plug-in configuration” on page 1489. **Distributed operating systems** **z/OS** For information about dynamic routing, see “Setting up dynamic routing for Liberty collectives” on page 1493 and “Generating a plugin-cfg.xml to route to multiple collectives” on page 1499.

**8.5.5.4** To configure an *auto scaling cluster*, which expands and contracts depending on the workload in your environment, see “Setting up auto scaling for Liberty collectives” on page 1503. Auto scaling clusters can receive requests only through dynamic routing.

---

## Chapter 3. Migrating applications to Liberty

You can migrate applications to Liberty.

### Procedure

Migrate data access applications to the Liberty profile.

---

### Migrating data access applications to Liberty

For data access applications, you need to change configurations when you migrate a data source from the WebSphere Application Server traditional to Liberty.

### Procedure

- “Configuration differences between the traditional and Liberty: dataSource and jdbcDriver elements.”
- “Configuration differences between the traditional and Liberty: connectionManager element” on page 1158.
- “Migrating a DB2 data source to Liberty” on page 1159.
- “Migrating a Derby embedded data source to Liberty” on page 1161.

### Configuration differences between the traditional and Liberty: dataSource and jdbcDriver elements

There are some differences in configuration between dataSource in Liberty and data sources in the traditional .

- Data source properties with different names
  - **ifxIFX\_LOCK\_MODE\_WAIT**, which is **informixLockModeWait** in traditional.
  - **supplementalJDBCTrace**, which is **supplementalTrace** in traditional.
  - **transactional**, which is **nonTransactionalDataSource** in traditional.
  - **isolationLevel**, which is **webSphereDefaultIsolationLevel** in traditional.
  - **queryTimeout**, which is **webSphereDefaultQueryTimeout** in traditional.
  - **id**, which is **name** in traditional.
- Data source properties with different values
  - **beginTranForResultSetScrollingAPIs**, which is true by default in Liberty
  - **beginTranForVendorAPIs**, which is true by default in Liberty
  - **connectionSharing**, which is MatchOriginalRequest by default in Liberty
  - **statementCacheSize**, which is is a JDBC provider property in traditional, and a **dataSource** property in Liberty, with a default value of 10.
- Data source properties in traditional that have no Liberty equivalent
  - **category**
  - **supportsDynamicUpdates**
- **connectionSharing** property of data sources
  - Liberty allows **connectionSharing** to be configured to either MatchOriginalRequest or MatchCurrentState. By default, it is **MatchOriginalRequest**.
  - The traditional allows **connectionSharing** to be configured in a finer grained manner, where individual connection properties can be matched based on the original connection request or the current state of the connection. In the traditional, **connectionSharing** is a combination of bits

representing which connection properties to match based on the current state of the connection. In the traditional, a value of 0 means to match all properties based on the original connection request; a value of -1 means to match all properties based on the current state of the connection. The default value for the traditional is 1, which means that the isolation level is matched based on the current state of the connection and all other properties are matched based on the original connection request.

- Time duration properties of data source

Time duration properties can optionally be specified with units in Liberty. For example,

```
<dataSource id="informix" jndiName="jdbc/informix" queryTimeout="5m" ...>
  <properties.informix ifxIFX_LOCK_MODE_WAIT="120s" .../>
</dataSource>
```

See for accepted time units and formats of dataSource element. Omitting the units in Liberty is equivalent to the default units used in the traditional.

- Configuration for JDBC drivers

- In Liberty, you can take the same approach of configuring different jdbcDriver elements for XA capable and non-XA capable data source implementation classes. Alternatively, you can use a single jdbcDriver element for both. Defining multiple jdbcDriver elements does not cause different class loaders to be used. In Liberty, jdbcDriver elements always use the class loader of the shared library with which they are configured.
- In the traditional, a JDBC provider is defined to point to the JDBC driver JARs, compressed files, and native files. You must define separate JDBC providers for XA capable and non-XA capable data source implementation classes.

For some of the commonly used JDBC drivers, Liberty infers the data source implementation class names based on the names the driver JARs. Therefore, you can omit the implementation class names. For example:

```
<jdbcDriver id="Derby" libraryRef="DerbyLib"/>
<library id="DerbyLib">
  <fileset dir="C:/Drivers/derby" includes="derby.jar" />
</library>
```

Use the optional properties of the default implementation classes to override these classes such as javax.sql.DataSource, javax.sql.ConnectionPoolDataSource, and javax.sql.XADataSource.

The following example shows how to override the default javax.sql.XADataSource and javax.sql.ConnectionPoolDataSource implementations that Liberty selects

```
<jdbcDriver id="Derby" libraryRef="DerbyLib"
  javax.sql.XADataSource="org.apache.derby.jdbc.EmbeddedXADataSource"
  javax.sql.ConnectionPoolDataSource="org.apache.derby.jdbc.EmbeddedConnectionPoolDataSource"/>
<library id="DerbyLib">
  <fileset dir="C:/Drivers/derby" includes="derby.jar" />
</library>
```

See for more information about the jdbcDriver element.

## Configuration differences between the traditional and Liberty: connectionManager element

There are some differences in configuration between connectionManager in Liberty and connection pools in the traditional.

- Properties with different names
  - **maxConnectionsPerThread**, which is **maxNumberOfMCSAllowableInThread** in the traditional.
  - **maxIdleTime**, which is **unusedTimeout** in the traditional.
  - **maxPoolSize**, which is **maxConnections** in the traditional.
  - **minPoolSize**, which is **minConnections** in the traditional.

- Time duration properties

You can optionally specify the time duration properties with units in Liberty. For example, `<connectionManager id="pool1" connectionTimeout="30s" reapTime="3m" maxIdleTime="30m"/>`

See for accepted time units and formats for the `connectionManager` element. If you do not specify time units in Liberty, the same default units are used as in the traditional.

- Differences between immediate timeout values and never (disable) timeout

There are differences in the values that represent immediate timeout and never (disabled) timeout.

- Liberty uses a value of 0 to represent immediate, whereas the traditional often uses -1 for immediate.
- Liberty uses a value of -1 to represent never (disabled), whereas the traditional often uses 0 for never (disabled).

Specifically this applies to the following attributes:

- **agedTimeout**
- **connectionTimeout**
- **maxIdleTime**, which is **unusedTimeout** in the traditional
- **reapTime**

- Purge policy changes

In Liberty, there are three purge policy values: **EntirePool**, **FailingConnectionOnly**, and **ValidateAllConnections**.

In the traditional, there are two purge policy values: **EntirePool** and **FailingConnectionOnly**, with a second property, `defaultPretestOptimizationOverride`, determining the behavior of **FailingConnectionOnly**.

Purge policies in Liberty, and their traditional equivalents, are as follows:

- `purgePolicy="EntirePool"`, which is the same for both.
- `purgePolicy="FailingConnectionOnly"`, which is equivalent to `purgePolicy="FailingConnectionOnly"` with `defaultPretestOptimizationOverride="false"` in the traditional.
- `purgePolicy="ValidateAllConnections"`, which is equivalent to `purgePolicy="FailingConnectionOnly"` with `defaultPretestOptimizationOverride="true"` in the traditional.

## Migrating a DB2 data source to Liberty

You can migrate a DB2 data source to Liberty.

### About this task

See the following code examples for the configurations for a DB2 data source in the traditional and Liberty.

### Example

In the traditional:

```
<resources.jdbc:JDBCProvider xmi:id="JDBCProvider_1321914412932"
    providerType="DB2 Using IBM JCC Driver" isolatedClassLoader="false"
    implementationClassName="com.ibm.db2.jcc.DB2ConnectionPoolDataSource" xa="false">
  <classpath>${DB2_JCC_DRIVER_PATH}/db2jcc4.jar</classpath>
  <classpath>${DB2_JCC_DRIVER_PATH}/db2jcc_license_cu.jar</classpath>
  <classpath>${DB2_JCC_DRIVER_PATH}/db2jcc_license_cisuz.jar</classpath>
  <factories xmi:type="resources.jdbc:DataSource" xmi:id="DataSource_1321914498985"
    name="DefaultDB2Datasource" jndiName="jdbc/DefaultDB2Datasource"
```

```

    providerType="DB2 Using IBM JCC Driver" authMechanismPreference="BASIC_PASSWORD"
    authDataAlias="IBM-9NE5C7ONIG4Node01/dbuser2" relationalResourceAdapter="builtin_rra"
    statementCacheSize="10"
    datasourceHelperClassname="com.ibm.websphere.rsadapter.DB2UniversalDataStoreHelper">
<propertySet xmi:id="J2EEResourcePropertySet_1321914499000">
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499000" name="databaseName"
    type="java.lang.String" value="TESTDB" required="true" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499001" name="driverType"
    type="java.lang.Integer" value="4" required="true" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499002" name="serverName"
    type="java.lang.String" value="localhost" required="false" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499003" name="portNumber"
    type="java.lang.Integer" value="50000" required="false" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499010" name="currentLockTimeout"
    type="java.lang.Integer" value="10" required="false" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499013" name="currentSchema"
    type="java.lang.String" value="DBUSER2" required="false" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499015" name="cursorSensitivity"
    type="java.lang.Integer" value="0" required="false" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499016" name="deferPrepares"
    type="java.lang.Boolean" value="true" required="false" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499027" name="loginTimeout"
    type="java.lang.Integer" value="0" required="false" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499032"
    name="resultSetHoldability" type="java.lang.Integer" value="1" required="false"
    ignore="false" confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499034"
    name="retrieveMessagesFromServerOnGetMessage"
    type="java.lang.Boolean" value="true" required="false" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499041" name="traceLevel"
    type="java.lang.Integer" value="-1" required="false" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499052"
    name="beginTranForResultSetScrollingAPIs" type="java.lang.Boolean" value="false"
    required="false" ignore="false" confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499053"
    name="beginTranForVendorAPIs" type="java.lang.Boolean" value="false" required="false"
    ignore="false" confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499054" name="connectionSharing"
    type="java.lang.Integer" value="-1" required="false" ignore="false"
    confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499060"
    name="nonTransactionalDataSource" type="java.lang.Boolean" value="false"
    required="false" ignore="false" confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499063"
    name="syncQueryTimeoutWithTransactionTimeout" type="java.lang.Boolean" value="false"
    required="false" ignore="false" confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499069"
    name="webSphereDefaultIsolationLevel" type="java.lang.Integer" value="2"
    required="false" ignore="false" confidential="false" supportsDynamicUpdates="false"/>
  <resourceProperties xmi:id="J2EEResourceProperty_1321914499070"
    name="webSphereDefaultQueryTimeout" type="java.lang.Integer" value="10"
    required="false" ignore="false" confidential="false" supportsDynamicUpdates="false"/>

```

```

    </propertySet>
    <connectionPool xmi:id="ConnectionPool_1321914499012" connectionTimeout="180"
        maxConnections="10" minConnections="1" reapTime="180" unusedTimeout="1800"
        agedTimeout="7200" purgePolicy="EntirePool" />
    <mapping xmi:id="MappingModule_1321914681786" mappingConfigAlias=""
        authDataAlias="IBM-9NE5C7ONIG4Node01/dbuser2"/>
</factories>
</resources.jdbc:JDBCProvider>
<systemLoginConfig xmi:id="JAASConfiguration_2">
    <authDataEntries xmi:id="auth1" alias="IBM-9NE5C7ONIG4Node01/dbuser2"
        userId="dbuser2" password="{xor}LDcfLTo70z0=" />
</systemLoginConfig>

```

In Liberty, the equivalent configuration is:

```

<variable name="DB2_JCC_DRIVER_PATH" value="C:/Drivers/DB2" />
<library id="db2Lib">
    <fileset dir="{DB2_JCC_DRIVER_PATH}" includes="db2jcc4.jar
        db2jcc_license_cu.jar db2jcc_license_cisuz.jar" />
</library>
<dataSource id="DefaultDB2Datasource" jndiName="jdbc/DefaultDB2Datasource"
    statementCacheSize="10"
    beginTranForResultSetScrollingAPIs="false"
    beginTranForVendorAPIs="false"
    connectionSharing="MatchCurrentState"
    transactional="false"
    syncQueryTimeoutWithTransactionTimeout="false"
    isolationLevel="TRANSACTION_READ_COMMITTED"
    queryTimeout="10"
    >
    <jdbcDriver libraryRef="db2Lib"
        javax.sql.ConnectionPoolDataSource="com.ibm.db2.jcc.DB2ConnectionPoolDataSource"/>
    <properties.db2.jcc
        databaseName="TESTDB"
        driverType="4"
        serverName="localhost"
        portNumber="50000"
        currentLockTimeout="10"
        currentSchema="DBUSER2"
        cursorSensitivity="0"
        deferPrepares="true"
        loginTimeout="0"
        resultSetHoldability="1"
        retrieveMessagesFromServerOnGetMessage="true"
        traceLevel="-1"
        user="dbuser2"
        password="{xor}LDcfLTo70z0="
    />
    <connectionManager connectionTimeout="180" maxPoolSize="10" minPoolSize="1" reapTime="180"
        maxIdleTime="1800" agedTimeout="7200" purgePolicy="EntirePool"/>
</dataSource>

```

## Migrating a Derby embedded data source to Liberty

You can migrate a Derby Embedded data source to Liberty.

### About this task

See the following code examples for the configurations for a Derby Embedded data source in the traditional and Liberty.

## Example

In the traditional:

```
<resources.jdbc:JDBCProvider xmi:id="JDBCProvider_1183122153343"
  providerType="Derby JDBC Provider"
  implementationClassName="org.apache.derby.jdbc.EmbeddedConnectionPoolDataSource"
  xa="false">
  <classpath>${DERBY_JDBC_DRIVER_PATH}/derby.jar</classpath>
  <factories xmi:type="resources.jdbc:DataSource" xmi:id="DataSource_1183122153625"
    name="DefaultDerbyDatasource" jndiName="jdbc/DefaultDatasource"
    providerType="Derby JDBC Provider" authMechanismPreference="BASIC_PASSWORD"
    relationalResourceAdapter="builtin_rra" statementCacheSize="10"
    datasourceHelperClassName="com.ibm.websphere.rsadapter.DerbyDataStoreHelper">
    <propertySet xmi:id="J2EEResourcePropertySet_1183122153625">
      <resourceProperties xmi:id="J2EEResourceProperty_1183122153625" name="databaseName"
        type="java.lang.String" value="C:/myDerby/DefaultDB" required="true"/>
      <resourceProperties xmi:id="J2EEResourceProperty_1183122153626" name="shutdownDatabase"
        type="java.lang.String" value="false" required="false"/>
      <resourceProperties xmi:id="J2EEResourceProperty_1183122153629" name="connectionAttributes"
        type="java.lang.String" value="upgrade=true" required="false"/>
      <resourceProperties xmi:id="J2EEResourceProperty_1183122153630" name="createDatabase"
        type="java.lang.String" value="create" required="false"/>
    </propertySet>
    <connectionPool xmi:id="ConnectionPool_1183122153625" connectionTimeout="180"
      maxConnections="10" minConnections="1" reapTime="180" unusedTimeout="1800"
      agedTimeout="7200" purgePolicy="EntirePool"/>
  </factories>
</resources.jdbc:JDBCProvider>
```

In Liberty, the equivalent configuration is:

```
<variable name="DERBY_JDBC_DRIVER_PATH" value="C:/Drivers/derby" />
<library id="derbyLib">
  <fileset dir="${DERBY_JDBC_DRIVER_PATH}" includes="derby.jar" />
</library>
<dataSource id="DefaultDerbyDatasource" jndiName="jdbc/DefaultDatasource"
  statementCacheSize="10">
  <jdbcDriver libraryRef="derbyLib"
    javax.sql.ConnectionPoolDataSource="org.apache.derby.jdbc.EmbeddedConnectionPoolDataSource"/>
  <properties.derby.embedded
    databaseName="C:/myDerby/DefaultDB"
    shutdownDatabase="false"
    connectionAttributes="upgrade=true"
    createDatabase="create"
  />
  <connectionManager connectionTimeout="180" maxPoolSize="10" minPoolSize="1" reapTime="180"
    maxIdleTime="1800" agedTimeout="7200" purgePolicy="EntirePool" />
</dataSource>
```

---

## Chapter 4. Installing Liberty

There are two methods for installing the WebSphere Application Server Liberty . You can use Installation Manager or use downloaded archive files. With either method, you can also download additional assets from the Liberty Repository.

### About this task

- | **New:** Liberty now follows a continuous delivery process with a new fix pack numbering scheme. Fix pack 16.0.0.2 is the next fix pack after 8.5.5.9. For more information about fix pack 16.0.0.2, see What is new in Liberty in the new location of the latest Liberty documentation.

When choosing installation methods, consider the packaging strategy of each method.

- For Installation Manager, you can download a single package that contains all requested content.
- For downloaded archive files, content is packaged in multiple archives to reduce download size.

The following table compares the available installation methods for WebSphere Application Server Liberty .

Table 90. Comparison of available installation methods

	Installation Manager	Archive
Agent-less installation	No	Yes
Install directly to any fix pack level	Yes	Yes
Apply fix packs in place	Yes	No
Apply interim fixes in place	Yes	Yes
Automated rollback of fix packs and interim fixes	Yes	No
Upgrade product editions	Yes	<b>8.5.5.5</b> Yes
Pluggable Java SDK provided	Yes	No
Integrated with developer tools	No	Yes
Add features in place	Yes	Yes
Liberty Repository integration	Yes	Yes
z/OS packaging provided	Yes	No
Minification supported	Yes, but the output of the minify command is a new image that can only be serviced with archive procedures.	Yes, the output of the minify command is a new image.

**z/OS** On the z/OS platform, installing the profile with downloaded archive files is not supported.

### Procedure

1. Install Liberty using one of the following methods:
  - a. Install Liberty using the Installation Manager.
  - b. Install Liberty using downloaded files and archives. You can install Liberty from a self-extracting Java archive file or a ZIP archive file.
2. Optional: Install assets from the Liberty Repository.

---

## Installing and uninstalling Liberty using Installation Manager

8.5.5.0

You can install WebSphere Application Server Liberty using IBM Installation Manager.

### About this task

**Note:** 8.5.5.11 Support for using Java SE 6 with WebSphere Liberty ends in September 2017. After the end of support, the Liberty kernel will be recompiled and can no longer run with Java SE 6. If you continue to use Java SE 6 on earlier fix packs after the end of support date, you could expose your environment to security risks.

Java SE 8 is the recommended Java SDK because it provides the latest features and security updates. You can install it by installing the IBM SDK, Java Technology Edition, Version 8 package to the package group that contains WebSphere Liberty.

Installation Manager is a general-purpose software installation and update tool that runs on a range of computer systems.

**Note:** Although WebSphere Application Server Liberty can be installed and maintained using Installation Manager Version 1.5.2 and later, this information is optimized for use with Installation Manager Version 1.6.2 and later. To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

**Note:** Starting with Version 1.6.2, Installation Manager supports Mac OS X. Installing and maintaining a Liberty offering using Installation Manager on Mac OS X is supported for the following offerings:

- IBM WebSphere Application Server Liberty
- IBM WebSphere Application Server Liberty Trial
- IBM WebSphere Application Server Liberty Core
- IBM WebSphere Application Server Liberty Core Trial
- IBM WebSphere Application Server Liberty - Express
- IBM WebSphere Application Server Liberty Network Deployment
- IBM WebSphere Application Server Liberty Network Deployment Trial
- IBM WebSphere Application Server Liberty for Developers
- IBM WebSphere Application Server Liberty for Developers (ILAN)

Installation Manager for Mac OS X is not contained in the product image or on the product media. You can obtain Installation Manager Version 1.6.2 and later from the IBM Installation Manager download website. Refer to the System Requirements for IBM Installation Manager website and System Requirements for WebSphere Application Server Version 8.5.5 website for complete details on Mac OS X support.

| **Note:** You can install WebSphere Application Server Liberty using the Installation Manager Graphical User Interface (GUI) or Installation Manager in console mode. Console mode is an interactive text-based user interface to Installation Manager. Use console mode when you do not have a graphics display device available or when you want to run the Installation Manager without the graphical user interface. For example, use console mode for server-side deployments when no graphical user interface is present, or for running the installation from a remote host.

| **New:** Liberty now follows a continuous delivery process with a new fix pack numbering scheme. Fix pack 16.0.0.2 is the next fix pack after 8.5.5.9. You can continue to use the same Version 8.5 Installation

Manager repositories and offering IDs to install or update to 16.0.0.2, or you can use the new versionless repositories and offerings. For more information about fix pack 16.0.0.2, see What is new in Liberty in the new location of the latest Liberty documentation.

Choose from the following options for more information on using Installation Manager for your installation.

## Procedure

- To install Liberty using Installation Manager, choose from the following options:
  - **Distributed operating systems** “Installing and uninstalling Liberty on distributed operating systems”
  - **IBM i** “Installing and uninstalling Liberty on IBM i operating systems” on page 1292
  - **z/OS** “Installing Liberty on z/OS” on page 1343
- **8.5.5.1** If you want to use Installation Manager in console mode, see: Installation Manager Version 1.6 documentation or the Installation Manager Version 1.5 documentation.

## Installing and uninstalling Liberty on distributed operating systems

### 8.5.5.0

IBM Installation Manager is a common installer for many IBM software products. You can use Installation Manager to install and manage the product lifecycle of WebSphere Application Server Liberty Network Deployment.

## Before you begin

Installation Manager is a single installation program that can use remote or local software flat-file repositories to install, modify, or update WebSphere Application Server products. It determines and shows available packages - including products, fix packs, interim fixes, and so on - checks prerequisites and interdependencies, and installs the selected packages. You also use Installation Manager to easily uninstall the packages that it installed.

### Restrictions:

- If you have an earlier Alpha or a Beta version of WebSphere Application Server Liberty Network Deployment installed, uninstall it before installing this version.
- **Windows** If a non-administrator installs WebSphere Application Server Liberty Network Deployment on a Windows Vista, Windows 7, or Windows Server 2008 operating system into the Program Files or Program Files (x86) directory with User Account Control (UAC) enabled, WebSphere Application Server Liberty Network Deployment will not function correctly.

UAC is an access-control mechanism that allows non-administrative users to install a software product into the Program Files or Program Files (x86) directory; but it then prohibits any write access to that directory after the installation has completed.

To resolve this issue, perform one of the following actions:

- Install the offering into a directory other than Program Files or Program Files (x86).

For example:

C:\IBM\WebSphere\Liberty

- Disable UAC.

- When you install an offering using Installation Manager with local repositories, the installation takes a significantly longer amount of time if you use a compressed repository file directly without extracting it.

Before you install an offering using local repositories, extract the compressed repository file to a location on your local system before using Installation Manager to access it.

**Important:** Do not transfer the content of a repository in non-binary mode and do not convert any content on extraction.

**Tip:** Although almost all of the instructions in this section of the documentation work with earlier versions of IBM Installation Manager, this information is optimized for users who installed or upgraded to Installation Manager Version 1.6.2 or later. Version 8.5.5.4 and later of Liberty require Installation Manager Version 1.6.2 or later.

- | **Tip:** Different users can use WebSphere Liberty by using two different methods.
- | 1. Install a new WebSphere Liberty instance for each user. Each WebSphere Liberty install is a new user profile.
- | 2. Create multiple servers with different users. Each user should be part of a group that has access to the wlpdirectory and java\_home used.
- | If you use option two, run the command to create the server as the user who will run the server and create the server in the user's home directory. If you are using Linux, the command is similar to `su user1 export WLP_USER_DIR=/home/user1 server create Server1`.
- | Setting WLP\_USER\_DIR in the user's shell profile makes it easy to ensure that all Liberty commands act on the correct user directory.

**Important:** Installation Manager can install any fix-pack level of the offering directly without installing the intermediate fix packs; in fact, Installation Manager installs the latest level by default. For example, you can skip fix-pack levels and go from Version 8.5.5.1 directly to Version 8.5.5.5. Keep in mind, however, that later you can not roll back to any level that was skipped. If you directly install to Version 8.5.5.5, for example, you cannot roll back to Version 8.5.5.4. If you skip from Version 8.5.5.1 to Version 8.5.5.5, you can only roll back to Version 8.5.5.1. You should plan your installations accordingly.

## About this task

Prepare your system as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.

Perform one of these procedures to install or uninstall WebSphere Application Server Liberty Network Deployment using Installation Manager.

## Procedure

- “Installing Liberty on distributed operating systems using the GUI” on page 1171
- “Installing Liberty on distributed operating systems by using the command line” on page 1174
- “Installing Liberty on distributed operating systems by using response files” on page 1178
- “Uninstalling Liberty from distributed operating systems using the GUI” on page 1188
- “Uninstalling Liberty from distributed operating systems using the command line” on page 1189
- “Uninstalling Liberty from distributed operating systems by using response files” on page 1189

## Results

### Notes on logging and tracing:

- An easy way to view the logs is to open Installation Manager and go to **File > View Log**. An individual log file can be opened by selecting it in the table and then clicking the **Open log file** icon.
- Logs are located in the logs directory of Installation Manager's application data location. For example:

- **Windows** **Administrative installation:**

C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager

- **Windows** **Non-administrative installation:**

C:\Documents and Settings\user\_name\Application Data\IBM\Installation Manager

- **AIX** **HP-UX** **Linux** **Solaris** **Administrative installation:**

/var/IBM/InstallationManager

- **AIX** **HP-UX** **Linux** **Solaris** **Non-administrative installation:**

user\_home/var/ibm/InstallationManager

- The main log files are time-stamped XML files in the logs directory, and they can be viewed using any standard web browser.
- The log.properties file in the logs directory specifies the level of logging or tracing that Installation Manager uses.

### Notes on troubleshooting:

- **HP-UX** When you attempt to launch Installation Manager from a DVD that was mounted using the CD-ROM file system (CDFS) on an HP-UX operating system, it might fail to launch and point to a log file that contains an exceptions similar to one of the following:

java.util.zip.ZipException: Exception in opening zip file:

org.osgi.framework.BundleException: Exception in  
org.eclipse.update.internal.configurator.ConfigurationActivator.start()  
or bundle org.eclipse.update.configurator.

This issue might be caused by Installation Manager reaching the upper limit of number of descriptors that can be opened on a CDFS-mounted device. This upper limit is determined by the value for the tunable kernel parameter ncdnode, which specifies the maximum number of CDFS nodes that can be in memory at any given time. To resolve the problem, change the ncdnode system kernel setting to 250. If the problem persists, increase the setting.

- **HP-UX** By default, some HP-UX systems are configured to not use DNS to resolve host names. This could result in Installation Manager not being able to connect to an external repository.

You can ping the repository, but nslookup does not return anything.

Work with your system administrator to configure your machine to use DNS, or use the IP address of the repository.

- In some cases, you might need to bypass existing checking mechanisms in Installation Manager.
  - On some network file systems, disk space might not be reported correctly at times; and you might need to bypass disk-space checking and proceed with your installation. To bypass disk-space checking, add `cic.override.disk.space=true` to the `config.ini` file in `IM_install_root/eclipse/configuration` and restart Installation Manager.
  - To bypass operating-system prerequisite checking, add `disableOSPrereqChecking=true` to the `config.ini` file in `IM_install_root/eclipse/configuration` and restart Installation Manager.

If you need to use any of these bypass methods, contact IBM Support for assistance in developing a solution that does not involve bypassing the Installation Manager checking mechanisms.

- For more information on using Installation Manager, read the IBM Installation Manager Information Center.

Read the release notes to learn more about the latest version of Installation Manager. To access the release notes, complete the following task:

- **Windows** Click **Start > Programs > IBM Installation Manager > Release Notes**.

- **AIX** **HP-UX** **Linux** **Solaris** Go to the documentation subdirectory in the directory where Installation Manager is installed, and open the `readme.html` file.

- If a fatal error occurs when you try to install the offering, take the following steps:

- Make a backup copy of your current installation directory in case IBM support needs to review it later.
- Use Installation Manager to uninstall everything that you have installed under the installation location (package group). You might run into errors, but they can be safely ignored.
- Delete everything that remains in the installation directory.
- Use Installation Manager to reinstall the offering to the same location or to a new one.
- **8.5.5.1** If you are installing WebSphere Application Server Liberty Version 8.5.5.1 in console mode, you might receive warning messages similar to the following example:

No "conClass" attribute in "commonPanel" element of panel com.ibm.was.liberty.userdata.panel.UserData in com.ibm.was.liberty.userdata.panel.

This problem is caused by an IBM Installation Manager API which is deprecated in Version 1.6.2. These warning messages can be ignored. No action is required.

## Installing Installation Manager and preparing to install Liberty

### 8.5.5.0

Install Installation Manager and obtain the necessary product repositories before installing WebSphere Application Server Liberty Network Deployment.

### About this task

To install Liberty, you must have Installation Manager Version 1.5.2 or later.

**Note:** **8.5.5.4** To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

### Procedure

#### 1. Install Installation Manager.

- a. Obtain the necessary installation files.

There are three basic options for obtaining Installation Manager Version 1.5.2 or later.

- **Access the physical media.**
- **Download the files from the Passport Advantage site.**

Licensed customers with a Passport Advantage ID and password can download Installation Manager from the Passport Advantage site.

**Tip:** See How to download WebSphere Application Server V8.5.5 from Passport Advantage Online.

- **Download the most current version of Installation Manager from the download website.**

You can download the most current version of Installation Manager from the IBM Installation Manager download website.

- b. Change to the location containing the Installation Manager installation files, and run one of the following commands.

#### Administrative installation:

- **Windows** `install.exe`
- **AIX** **HP-UX** **Linux** **Solaris** `./install`

#### Non-administrative installation:

- **Windows** `userinst.exe`
- **AIX** **HP-UX** **Linux** **Solaris** `./userinst`

## Group-mode installation:

**AIX** **HP-UX** **Linux** **Solaris** `./groupinst`

### Notes® on group mode:

- Group mode allows multiple users to use a single instance of IBM Installation Manager to manage software packages.  
This does not mean that two people can use the single instance of IBM Installation Manager at the same time.
- **Windows** Group mode is not available on Windows operating systems.
- If you do not install Installation Manager using group mode, you will not be able to use group mode to manage any of the products that you install later using this Installation Manager.
- Make sure that you change the installation location from the default location in the current user's home directory to a location that is accessible by all users in the group.
- Set up your groups, permissions, and environment variables as described in the Group mode road maps in the IBM Installation Manager documentation before installing in group mode.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager documentation.

The installer opens an **Install Packages** window.

c. Make sure that the Installation Manager package is selected, and click **Next**.

d. Accept the terms in the license agreements, and click **Next**.

The program creates the directory for your installation.

e. Click **Next**.

f. Review the summary information, and click **Install**.

- If the installation is successful, the program displays a message indicating that installation is successful.
- If the installation is not successful, click **View Log File** to troubleshoot the problem.

## 2. Update an Installation Manager installation that is already on your system.

For information on updating Installation Manager to Version 1.5.2 or later, see the IBM Installation Manager documentation.

## 3. Obtain the product repositories.

There are three basic options for accessing the product repositories to install the offering.

- **Access the physical media, and use local installation.**

You can access the product repositories on the media.

- **Download the files from the Passport Advantage site, and use local installation.**

Licensed customers with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

**Tip:** See How to download WebSphere Application Server V8.5.5 from Passport Advantage Online for a list of the IBM WebSphere Application Server Liberty Network Deployment installation images downloadable from the IBM Passport Advantage Online website and other information.

- **Access the live repositories, and use web-based installation.**

If you have a Passport Advantage ID and password, you can access the product repositories and install the offering from the web-based repositories. Use Installation Manager to install the offering from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85>

**Note:** This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must add to your Installation Manager preferences before the Installation Manager GUI can access the files in this repository to install the offering.

**Tip:** This live repository is accessed by using Passport Advantage authentication. After you have installed Installation Manager, you can set the Passport Advantage preference to connect to the live repositories. To set Passport Advantage preferences, follow this procedure:

- a. Open Installation Manager.
- b. Open the Passport Advantage preferences page by selecting **File > Preferences > Passport Advantage**.
- c. Select **Connect to Passport Advantage** to connect to the Passport Advantage repository.  
The Password Required dialog box opens.
- d. Enter a user name and password for Passport Advantage.
- e. **Optional:** Select **Save password** to save the user name and password credentials.  
If you do not save the user name and password credentials, you are prompted for these credentials each time you access Passport Advantage.
- f. Click **OK** to close the Password Required dialog box.
- g. Click **OK** to close the Preferences window.

For more information on setting your Installation Manager preferences, see the IBM Installation Manager documentation.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

**Notes:**

- If you do not have a Passport Advantage ID and password, you must install the offering from the product repositories on the media or local repositories.
- With the Packaging Utility, you can create and manage packages for installation repositories. You can copy multiple packages into one repository or copy multiple disks for one product into a repository. You can copy packages from Passport Advantage or a web-based repository into a local repository for example. For more information on the Packaging Utility, go to the IBM Installation Manager documentation.

4.   Optional: Configure an instance of the Liberty Asset Repository Service or a local directory-based repository.

As part of installing Liberty, you can choose to install assets from the following repositories:

- The IBM WebSphere Liberty Repository, a public IBM-hosted repository that is accessible through the internet. For more information, see “Liberty: Liberty Repository” on page 965.
- The Liberty Asset Repository Service, an open-source service that you can use to create an on-premises repository that is remotely accessible behind the firewall of an enterprise. For more information, see the WASdev/tool.lars project on GitHub.
- Local directory-based repositories that are created by using the **installUtility download** action. For more information, see “Downloading assets using the installUtility command” on page 1400.

Access to the IBM WebSphere Liberty Repository is enabled by default and requires internet access. If your system does not have internet access or you want to install customized Liberty assets, set up an instance of the Liberty Asset Repository Service or a local directory-based repository, and then add the repository in Installation Manager. For more information about the Liberty repositories, see “Installing assets using Installation Manager” on page 1411.

5. **Optional: If you will be using the Installation Manager GUI, add repositories to your Installation Manager preferences.**
- a. Launch Installation Manager.
  - b. Click **File > Preferences**.

- c. Select **Repositories**.
- d. Perform the following actions:
  - 1) Click **Add Repository**.
  - 2) Enter the path to the repository.config file in the location containing the repository files.

For example:

- Windows C:\repositories\offering\_name\local-repositories
- AIX HP-UX Linux Solaris /var/repositories/offering\_name/local-repositories

or

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85>

- 3) Click **OK**.
- e. Deselect any locations listed in the Repositories window that you will not be using.
- f. Click **Apply**.
- g. Click **OK**.
- h. Click **File > Exit** to close Installation Manager.

For more information on setting your Installation Manager preferences, see the IBM Installation Manager documentation.

## 6. Optional: If you will be using the Installation Manager GUI, set your Installation Manager rollback preferences.

By default, Installation Manager saves earlier versions of a package to roll back to if you experience issues later. When Installation Manager rolls back a package to a previous version, the current version of the files are uninstalled and the earlier versions are reinstalled. If you choose not to save the files for rollback, you can prevent the files from being saved or delete them after they are saved. To set your rollback preferences, perform the following actions before installing a package:

- a. Launch Installation Manager.
- b. Open the Rollback preferences window by selecting **File > Preferences > Files for Rollback**.
- c. Select or clear the **Save files for rollback** option to save or to stop saving a copy of files that are required to roll back packages on your computer.

You can remove any files that have already been saved by clicking **Delete Saved Files**. If you delete the files and you need to roll back a package later, you must connect to a repository or insert the media to obtain the required files for the previous version of the package.

- d. Click **OK** to save your rollback preferences.

For more information on setting your Installation Manager preferences, see the IBM Installation Manager documentation.

## What to do next

Use Installation Manager to install the offering.

- “Installing Liberty on distributed operating systems using the GUI”
- “Installing Liberty on distributed operating systems by using the command line” on page 1174
- “Installing Liberty on distributed operating systems by using response files” on page 1178

## Installing Liberty on distributed operating systems using the GUI

**8.5.5.0**

You can use the Installation Manager GUI to install WebSphere Application Server Liberty Network Deployment.

## Before you begin

Prepare your system as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.

## About this task

**8.5.5.4** To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

## Procedure

1. Start Installation Manager.

**Tip:** **AIX** **HP-UX** **Linux** **Solaris** You can start Installation Manager in group mode with the `./IBMIM` command.

- Group mode allows multiple users to use a single instance of IBM Installation Manager to manage software packages.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager documentation.

2. Click **Install**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

Installation Manager searches its defined repositories for available packages.

3. Perform the following actions.

- a. Select **IBM WebSphere Application Server Liberty Network Deployment** and the appropriate version.

**Note:** If you are installing the trial version of this product, select the appropriate trial edition and the appropriate version.

If you already have the WebSphere Application Server Liberty Network Deployment offering installed on your system in the installation location, a message displays indicating that the product is already installed. To create another installation of the offering in another location, click **Continue**.

**Tip:** If the **Search service repositories during installation and updates** option is selected on the Installation Manager Repository preference page and you are connected to the Internet, you can click **Check for Other Versions and Extensions** to search for updates in the default update repositories for the selected packages. In this case, you do not need to add the specific service-repository URL to the Installation Manager Repository preference page.

- b. Select the fixes to install.

Any recommended fixes are selected by default.

If there are recommended fixes, you can select the option to show only recommended fixes and hide non-recommended fixes.

- c. Click **Next**.

**Note:** Installation Manager might prompt you to update to the latest level of Installation Manager when it connects to the repository. Update to the newer version before you continue if you are prompted to do so. Read the IBM Installation Manager documentation for information about automatic updates.

4. Accept the terms in the license agreements, and click **Next**.

5. Specify the installation root directory for the product binaries, which are also referred to as the core product files or system files.

The panel also displays the shared resources directory and disk-space information.

**Note:** The first time that you install a package using Installation Manager, you can specify the shared resources directory. The shared resources directory is where installation artifacts are located that can be used by one or more package groups. It is also used as a staging area for the product payload during installation operations. By default, this content is cached so that it can be used for rollback. Consider setting your rollback preferences to save these files as described in “Installing Installation Manager and preparing to install Liberty” on page 1168. Use your largest drive for this installation. You cannot change the directory location until after you uninstall all packages.

If you are installing on a 64-bit system, use the bit-selection option to select the bitness of the installed Java libraries. If you are installing on a 32-bit system, this option is not available. When installing on a 64-bit system, you must select either the 32-bit or 64-bit option. This choice will determine the architecture bitness of the installation profile group. All extension offerings to WebSphere Application Server Liberty Network Deployment will be installed under the same profile group and have the same architecture bitness. For example, WebSphere SDK Java Technology Edition Version 7.0 for Liberty is an extension offering to WebSphere Application Server Liberty Network Deployment and its installation will use a 32-bit or 64-bit JDK depending on your choice here.

#### Restrictions:

- Deleting the default target location and leaving an installation-directory field empty prevents you from continuing.
- Do not use symbolic links as the destination directory.  
Symbolic links are not supported.
- Do not use a semicolon in the directory name.

WebSphere Application Server Liberty Network Deployment cannot install properly if the target directory includes a semicolon.

 A semicolon is the character used to construct the class path on Windows systems.

6. Click **Next**.
7. Select the features that you want to install.

Choose from the following features:

- IBM WebSphere Application Server Liberty Network Deployment
  - Embeddable EJB container and JPA client

This option installs the embeddable EJB container and JPA client.

The embeddable EJB container is a Java Archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition (SE) environment. You can run enterprise beans using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.

The JPA client can be used with the embeddable EJB container to provide Java Persistence API capability in a Java SE environment.

**Tip:** You can run Installation Manager later to modify this installation and add or remove this feature.

- Extended Programming Models (Versions 8.5.5.0 to 8.5.5.3)

The Extended Programming Models feature provides a rich set of programming models such as Web Services, JMS (including Message-Driven Beans), and MongoDB 2.0.



8.5.5.4

Beginning with Version 8.5.5.4, the Extended Programming Models are available from the Liberty Repository. This asset provides a rich set of programming models such as Web

Services, JMS (including Message-Driven Beans), and MongoDB 2.0. To install this asset, use the Asset Selection Wizard as described in later steps.

8. Click **Next**.

9.  **8.5.5.2** Optional: Install additional Liberty Repository assets. If you do not want to select any additional assets, you can skip this step. To install Liberty Repository assets, you must have IBM Installation Manager Version 1.6.2 or later. To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.

a. Select whether you want to install assets from the Liberty Repository, and click **Next**. To install assets from the IBM WebSphere Liberty Repository, you must have access to the internet.

**8.5.5.6** If you choose not to connect to the IBM WebSphere Liberty Repository, you can still install assets from configured directory-based repositories or an instance of the Liberty Asset Repository Service. For more information, see “Installing assets using Installation Manager” on page 1411.

b. **8.5.5.4** Click **Launch Asset Selection Wizard**.

c. You can perform a case-insensitive search for assets by display name or description. If you search with the **Keyword** field empty, then the search displays all applicable assets.

**8.5.5.5** With Version 8.5.5.5 and later, you can also search for assets by short name.

d. Select each asset that you want to install, then click **Next**.

e. Accept the license agreement and click **Finish**.

10. Click **Next**.

11. Review the summary information, and click **Install**.

- If the installation is successful, the program displays a message indicating that installation is successful. The program might also display important post-installation instructions.
- If the installation is not successful, click **View Log File** to troubleshoot the problem.

12. Click **Finish**.

13. Click **File > Exit** to close Installation Manager.

## Installing Liberty on distributed operating systems by using the command line

### **8.5.5.0**

You can install WebSphere Application Server Liberty Network Deployment by using the Installation Manager command line.

### Before you begin

**Important:** Before you install WebSphere Application Server Liberty Network Deployment, you must read the license agreement that you can find with the product files. Signify your acceptance of the license agreement by specifying `-acceptLicense` in the command as described in this topic.

Prepare the system onto which you want to install WebSphere Application Server Liberty Network Deployment as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.

### About this task

**8.5.5.4** To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

### Procedure

1. Optional: If the repository requires a user name and password, create credential-storage and master-password files to access this repository.

**Tip:** When you create a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, use the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the `-keyring` and `-password` options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the `-keyring` and `-password` options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

2. Log on to your system.
3. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
4. Verify that the offering repository is available.

Windows

```
imcl.exe listAvailablePackages -repositories source_repository
```

AIX

HP-UX

Linux

Solaris

```
./imcl listAvailablePackages -repositories source_repository
```

You see one or more levels of the offering.

5. Use the `imcl` command to install the offering.

Windows

```
imcl.exe install com.ibm.websphere.liberty.ND.v85_offering_version,optional_feature_ID  
-repositories source_repository  
-installationDirectory installation_directory  
-sharedResourcesDirectory shared_directory  
-preferences preference_key=value  
-properties property_key=value  
-secureStorageFile storage_file -masterPasswordFile master_password_file  
-acceptLicense
```

AIX

HP-UX

Linux

Solaris

```
./imcl install com.ibm.websphere.liberty.ND.v85_offering_version,optional_feature_ID  
-repositories source_repository  
-installationDirectory installation_directory  
-sharedResourcesDirectory shared_directory  
-preferences preference_key=value  
-properties property_key=value  
-secureStorageFile storage_file -masterPasswordFile master_password_file  
-acceptLicense
```

### Tips:

- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lafiles` or `offering_name/lafiles` subdirectory of the installation image or repository for this offering.
- The first time that you install a package by using the Installation Manager, you can specify the shared resources directory. The shared resources directory is where installation artifacts are located that can be used by one or more package groups. It is also used as a staging area for the product payload during installation operations. By default, this content is cached so that it can be used for rollback. Use your largest drive for this installation. You cannot change the directory location until after you uninstall all packages.
- The `offering_version`, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.5.20110503\_0200 for example).
  - If `offering_version` is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If `offering_version` is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the `-installFixes` option defaults to all.
  - If the offering version is specified, the `-installFixes` option defaults to none.
- You can add a list of features that are separated by commas:
  - Embeddable EJB container and JPA client (`embeddablecontainer`)  
This option installs the embeddable EJB container and JPA client.  
The embeddable EJB container is a Java Archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition (SE) environment. You can run enterprise beans by using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.  
The JPA client can be used with the embeddable EJB container to provide Java Persistence API capability in a Java SE environment.
  - Extended Programming Models (`extprogmodels`) - Versions 8.5.5.0 to 8.5.5.3  
The Extended Programming Models feature provides a rich set of programming models such as Web Services, JMS (including Message-Driven Beans), and MongoDB 2.0.

#### Notes:

- If no features are specified, the default features (`embeddablecontainer` and `extprogmodels` Version 8.5.5.3 and previous) are installed. To install only the feature that you want, specify that feature explicitly.



8.5.5.4

Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` addon, or install the individual features that you need from the Liberty Repository. See the following topics for more information:

- Installing Liberty Repository assets
- Liberty features
- To ensure that your installation process completes for systems that do not have internet access specify the `-properties user.feature=""` parameter on the Installation Manager command line. If you do not specify this parameter, the installation process attempts to access the internet and an error occurs.  
ERROR: Unable to connect to the IBM WebSphere Liberty repository or local Installation Manager repository.

Verify that firewalls are configured to allow the Installation Manager to access the internet, or that the local Installation Manager repository can be accessed. If the problem persists, then the repository server might be unavailable. To continue the installation without additional assets, specify the `user.feature=""` and `user.addon=""` parameters.

- 8.5.5.5

You can receive a `NullPointerException` when you apply fix pack V8.5.5.5 for WebSphere Application Server Liberty. The error can occur when you download the WebSphere Application Server Liberty fix pack compressed files and use them, at the downloaded directory location, to install or update Liberty. You can work around this Version 8.5.5.5 error condition by taking the following steps:
- Extract the WebSphere Application Server Liberty fix pack compressed file to a temporary directory.
- Use the temporary directory as the Installation Manager repositories to install or update Liberty.

```

unzip 8.5.5-WS-LIBERTYPROFILE-OS390-FP0000005.zip to /tmp/fp8555
# ./imcl install
com.ibm.websphere.liberty.v85_8.5.5005.20150305_2214
-installationDirectory /SERVICE/usr/lpp/zWebSphere/Liberty/V8R5
-repositories
/tmp/fp8555
-acceptLicense

```

- 
**8.5.5.2** You can specify additional assets to install from the Liberty Repository. For a list of Liberty Repository assets, see the downloads page on WASdev.net. If you want to install additional assets, specify the following properties on the command line. You can specify the short name or symbolic name. Note that the feature short names, such as *FeatureA*, are separated by double commas in the following example:

```
-properties user.feature=FeatureA,,FeatureB,,FeatureC,user.accept.license=true
```

**8.5.5.5** For Version 8.5.5 and later, `user.accept.license=true` is not required.

- 
**8.5.5.4** The following example installs the Extended Programming Models on the `user.addon` parameter, and the Portlet Container feature on the `user.feature` parameter.

```

imcl install com.ibm.websphere.liberty.ND.v85
-properties user.accept.license=true,user.addon=extendedPackage-1.0,user.feature=portlet-2.0
-installationDirectory D:\IBM\Liberty -acceptLicense
-repositories D:\IBM\LibertyRepo
-sharedResourcesDirectory D:\IBM\IMShared
-showProgress

```

- 
**8.5.5.6** You can also install assets from instances of the Liberty Asset Repository Service or local directory-based repositories. For more information about these asset repositories, see “Installing assets using Installation Manager” on page 1411. Add the repository on the `-repositories` parameter. The repositories are accessed in the order that they are specified. By default, the Liberty Repository is the last of the repositories that are accessed during installation. To disable access to the Liberty Repository, on the `-properties` parameter, set the `user.useLibertyRepository` option to `false`.

```

imcl install com.ibm.websphere.liberty.ND.v85
-properties user.useLibertyRepository=false,user.addon=extendedPackage-1.0,user.feature=portlet-2.0
-installationDirectory D:\IBM\Liberty -acceptLicense
-repositories D:\IBM\LibertyProductRepo,https://your_onprem_asset_repo_url,D:\IBM\LocalAssetRepo,D:\IBM\LocalAssetRepo2.zip
-sharedResourcesDirectory D:\IBM\IMShared
-showProgress

```

To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.

- Installation Manager can save earlier versions of a package to roll back to if you experience issues later. When Installation Manager rolls back a package to a previous version, the current versions of the files are uninstalled and the earlier versions are reinstalled. If you choose not to save the files for rollback, you can prevent the files from being saved by using the following preference in your command specification:

```
-preference com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts=False
```

For more information on setting your Installation Manager preferences, see IBM Installation Manager documentation.

**Tip:** Even if you choose not to preserve files locally for rollback, you can still roll back to any previously installed level by accessing the appropriate offering repository.

- You can use the `cic.selector.arch` property key and related value to specify the architecture to install, 32 bit or 64 bit.

Here is an example of specifying a 32-bit architecture:

```
-properties cic.selector.arch=x86
```

If you do not specify anything for this key, you get a correct match for your system. For a 64-bit system, the installation defaults to a 64-bit installation.

Your choice here applies to all packages that are installed in the package group. For information about the supported values for the `cic.selector.key` keys, see the Values for `cic.selector.key` table in the Installation Manager documentation.

- The program might write important post-installation instructions to standard output.

For more information on using the `imcl` command to install the offering, see the IBM Installation Manager documentation.

## Installing Liberty on distributed operating systems by using response files

8.5.5.0

You can install WebSphere Application Server Liberty Network Deployment by using Installation Manager response files.

### Before you begin

Prepare each of the systems onto which you want to install the offering as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.

### About this task

Using Installation Manager, you can work with response files to install the offering in various ways. You can record a response file by using the GUI as described in the following procedure, create a new response file, or copy and modify an existing response file.

8.5.5.4 To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

### Procedure

1. Optional: Record a response file to install the offering.

On one of your systems, perform the following actions to record a response file that can install the offering.

- a. From a command line, change to the `eclipse` subdirectory in the directory where you installed Installation Manager.
- b. Start Installation Manager from the command line by using the `-record` option.

For example:

- **Windows** Administrator or non-administrator:

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"  
-record C:\temp\install_response_file.xml
```

- **AIX** **HP-UX** **Linux** **Solaris** Administrator:

```
./IBMIM -skipInstall /var/temp/imRegistry  
-record /var/temp/install_response_file.xml
```

- **AIX** **HP-UX** **Linux** **Solaris** Non-administrator:

```
./IBMIM -skipInstall user_home/var/temp/imRegistry  
-record user_home/var/temp/install_response_file.xml
```

**Tip:** When you record a new response file, you can specify the `-skipInstall` parameter. Using this parameter has the following benefits:

- No files are installed, which speeds up the recording.
- If you use a temporary data location with the `-skipInstall` parameter, Installation Manager writes the installation registry to the specified data location while recording. When you start Installation Manager again without the `-skipInstall` parameter, you then can use your response file to install against the real installation registry.

Do not use the **-skipInstall** operation on the agent data location that is used by Installation Manager. This operation is unsupported. Use a clean writable location, and reuse that location for future recording sessions.

For more information, read the IBM Installation Manager documentation.

- c. Follow the instructions that are described in “Installing Liberty on distributed operating systems using the GUI” on page 1171.
2. Optional: Create a credential-storage file for installation. If you are using an authenticated remote repository, you can store credentials for URLs that require authentication, such as remote repositories, in a credential-storage file. For IBM Installation Manager Version 1.6.2 and later, use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. For previous versions of Installation Manager, the **-keyring** and **-password** options are used to access credentials in a keyring file. These options are deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures.
  - For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation.
  - For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.
3. Use the response files to install the offering.

Go to a command line on each of the systems on which you want to install the offering, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the offering.

For example:

- **Windows** Administrator or non-administrator:

```
imcl.exe -acceptLicense
input C:\temp\install_response_file.xml
-log C:\temp\install_log.xml
-secureStorageFile C:\IM\credential.store -masterPasswordFile C:\IM\master_password_file.txt
```

- **AIX** **HP-UX** **Linux** **Solaris** Administrator:

```
./imcl -acceptLicense
input /var/temp/install_response_file.xml
-log /var/temp/install_log.xml
-secureStorageFile /var/IM/credential.store -masterPasswordFile /var/IM/master_password_file.txt
```

- **AIX** **HP-UX** **Linux** **Solaris** Non-administrator:

```
./imcl -acceptLicense
input user_home/var/temp/install_response_file.xml
-log user_home/var/temp/install_log.xml
-secureStorageFile user_home/var/IM/credential.store -masterPasswordFile user_home/var/IM/master_password_file.txt
```

#### Notes:

- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lafiles` or `offering_name/lafiles` subdirectory of the installation image or repository for this offering.
- The program might write important post-installation instructions to standard output.

Read the IBM Installation Manager documentation for more information.

## Example

**Windows** The following is an example of a response file for installing the offering.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean="true" temporary="true">
<server>
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85" />
</server>
<install modify='false'>
<offering id='com.ibm.websphere.liberty.ND.v85'
profile='WebSphere Liberty V8.5'
features='embeddablecontainer' installFixes='none' />
</install>
```

```
<profile id='WebSphere Liberty V8.5'
  installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
</agent-input>
```

**Important:** AIX Linux Solaris Windows If you are installing on a 64-bit system, you must include one of the options for an IBM Software Development Kit.

- You can use the `cic.selector.arch` property key and related value to specify the architecture to install, 32 bit or 64 bit.

Here is an example of specifying a 32-bit architecture:

```
<profile>
...
<data key='cic.selector.arch' value='x86' />
...
</ptofile>
```

If you do not specify anything for this key, you receive a correct match for your system. For a 64-bit system, the installation defaults to a 64-bit installation.

Your choice here applies to all packages that are installed in the package group. For information about the supported values for the `cic.selector.key` keys, see the Values for `cic.selector.key` table in the Installation Manager documentation.

To disable remote searches for updates in the response file, set the following preferences to false:

- **offering.service.repositories.areUsed**  
Used for searching remote repositories for updates to installed offerings
- **com.ibm.cic.common.core.preferences.searchForUpdates**  
Used for searching for updates to Installation Manager

For example:

```
<preference value='false' name='offering.service.repositories.areUsed' />
<preference value='false' name='com.ibm.cic.common.core.preferences.searchForUpdates' />
```

You can find more details on silent preference keys in the IBM Installation Manager documentation.

The following examples show you how to change response file in order to perform alternative actions.

- To install multiple copies of this offering, specify a different installation location and a new package group for each installation. For example, to install a second copy of the offering into the `C:\Program Files\IBM\WebSphere\Liberty_2` directory and create the WebSphere Liberty V8.5\_2 package group, replace:

```
<profile id='WebSphere Liberty V8.5'
  installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
```

with:

```
<profile id='WebSphere Liberty V8.5_2'
  installLocation='C:\Program Files\IBM\WebSphere\Liberty_2'>
```

- To add optional features, add them as an entry in a comma-separated list. For example:

```
<offering id='com.ibm.websphere.liberty.ND.v85'
  profile='WebSphere Liberty V8.5'
  features='embeddablecontainer,extprogmodes' installFixes='none' />
```

- Embeddable EJB container and JPA client (`embeddablecontainer`)

This option installs the embeddable EJB container and JPA client.

The embeddable EJB container is a Java archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition (SE) environment. You can run enterprise beans by using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.

The JPA client can be used with the embeddable EJB container to provide Java Persistence API capability in a Java SE environment.

- Extended Programming Models (extprogmodels) Versions 8.5.5.0 to 8.5.5.3

The Extended Programming Models feature provides a rich set of programming models such as Web Services, JMS (including Message-Driven Beans), and MongoDB 2.0.

 **8.5.5.4** Beginning with Version 8.5.5.4, the Extended Programming Models are available from the Liberty Repository. To install Liberty Repository assets, see the information later in this section.

If no features are specified, the default features (embeddablecontainer and extprogmodels) are installed. To install only the feature that you want, specify that feature explicitly.

-  **8.5.5.2** You can specify additional assets to install from the Liberty Repository. For a list of Liberty Repository assets, see the downloads page on WASdev.net.

To install Liberty Repository assets, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later. Previous versions of Installation Manager do not have the option to install Liberty Repository assets. If you use a response file and did not update Installation Manager to Version 1.6.2 or later, the assets that you specify in the response file are ignored during installation.

If you want to install additional features, specify two extra data key elements in your response file. You can use either the symbolic name or the short name.

The following example installs the Portlet Container and Portlet Serving features using the symbolic name.

```
<data key='user.feature' value='com.ibm.websphere.appserver.portlet-2.0,,com.ibm.websphere.appserver.portletserving-2.0' />
<data key='user.accept.license' value='true' />
```

The following example installs the Portlet Container and Portlet Serving features using the short name:

```
<data key='user.feature' value='portlet-2.0,,portletserving-2.0' />
<data key='user.accept.license' value='true' />
```

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.

 **8.5.5.4** Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` addon, or install the individual features that you need from the Liberty Repository. See the following topics for more information:

- Installing Liberty Repository assets
- Liberty features

The following example installs the Extended Programming Models using the `user.addon` parameter and the Portlet Container and Portlet Serving features using the `user.feature` parameter with short names:

```
<data key='user.addon' value='extendedPackage-1.0' />
<data key='user.feature' value='portlet-2.0,,portletserving-2.0' />
<data key='user.accept.license' value='true' />
```

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.

 **8.5.5.6** You can also install assets from an instance of the Liberty Asset Repository Service or local directory-based repositories. For more information, see “Installing assets using Installation Manager” on page 1411. Add the repository on repository elements. If Installation Manager does not recognize the repository, point directly to the repository.config file. When you install assets, the repositories are accessed in the order that you specify them.

```
<server>
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85" />
<repository location="https://your_onprem_asset_repo_url" />
<repository location="D:\IBM\LocalAssetRepo" />
```

**8.5.5.8** `<repository location="D:\IBM\LocalAssetRepo2.zip" /> </server>` By default, the Liberty Repository is the last of the repositories that are accessed during installation. To disable access to the Liberty Repository, set the `user.useLibertyRepository` parameter to false:

```
<data key='user.addon' value='extendedPackage-1.0' />
<data key='user.feature' value='portlet-2.0,,portlet-serving-2.0' />
<data key='user.useLibertyRepository' value='false' />
```

To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.

- Installation Manager can save earlier versions of a package to roll back to if you experience issues later. When Installation Manager rolls back a package to a previous version, the current versions of the files are uninstalled and the earlier versions are reinstalled. If you choose not to save the files for rollback, you can prevent the files from being saved by changing the following preference in your response file:

```
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
```

to this:

```
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='false' />
```

For more information on setting your Installation Manager preferences, see the IBM Installation Manager documentation.

**Tip:** Even if you choose not to preserve files locally for rollback with this option, you can still roll back to any previously installed level by accessing the appropriate product repository.

## Updating Liberty from Version 8.5.0 to Version 8.5.5

Distributed operating systems

IBM i

8.5.5.0

If you are updating an existing WebSphere Application Server Version 8.5.0.x Liberty feature, you must install WebSphere Application Server Liberty Network Deployment Version 8.5.5.0 or later. You cannot make an in-place update of the Version 8.5.0.x Liberty feature. Afterwards, you can copy your data and server configurations to the new installation or, if your user data are kept in another location, follow typical procedures for managing your data and server configurations.

### About this task

In WebSphere Application Server Version 8.5.5.0, Liberty was promoted from a feature to an independently installable offering. You cannot make an in-place update of the Version 8.5.0.x Liberty feature. The `wlp` folder includes the Liberty runtime and any user data or server configurations that you have saved in the `wlp/usr` folder. If you have a combined full-profile and Liberty-profile Version 8.5.0.x installation, the update program will back up the `wlp` folder for the existing Version 8.5.0.x Liberty feature into the `wlp.bak_<timestamp>` folder and uninstall the feature during an update to Version 8.5.5.0 or higher. You can continue using Liberty from the backed-up location or copy it elsewhere. To update Liberty to Version 8.5.5.0 or higher, you then must install WebSphere Application Server Liberty Network Deployment (with the `com.ibm.websphere.liberty.ND.v85` offering ID). After installing WebSphere Application Server Liberty Network Deployment, you can move any user data and server configurations from the `wlp.bak_<timestamp>` folder to the new Liberty installation.

These instructions describe updating from a combined full-profile and Liberty-profile Version 8.5.0.x installation. If you have only the Version 8.5.0.x Liberty feature installed, you should install WebSphere Application Server Liberty Network Deployment Version 8.5.5.0 or higher in a different location. Then, you can copy the contents of the `wlp/usr` directory from the old installation to the `usr` directory of the new installation. If you are using `WLP_USER_DIR` and `WLP_OUTPUT_DIR` environment variables, make sure that they are pointing to the desired locations. You can continue using Java 6 from the Version 8.5.0.x installation image, use your own Java 6 or Java 7 that meets Liberty minimum requirements, or install one or both of the optional Java 6 or Java 7 Liberty extension offerings (offering ids: `com.ibm.websphere.liberty.IMBJAVA.v60` and `com.ibm.websphere.liberty.IMBJAVA.v70`).

**Note:**  During installation of a Liberty offering on an IBM i system, the `WLP_DEFAULT_USER_DIR` and `WLP_DEFAULT_OUTPUT_DIR` environment variables are set in the `WLP_INSTALL_DIR/etc/default.env` file.

## Procedure

1. Update your existing combined full-profile and Liberty-profile installation to Version 8.5.5 or later following the normal update procedure.

**Note:** If you want to keep using the backed-up Liberty with the current level of Java 6 after the update, you must make a backup of Java 6 before it is updated to the latest level by the fix-pack update. Java 6 can be found in the `<install-root>\java` folder. Set the `JAVA_HOME` environment variable to point to the desired Java. For more information on this environment variable, see “Customizing the Liberty environment” on page 1565.

After updating your WebSphere Application Server Network Deployment installation from Version 8.5.0.x to Version 8.5.5, you can find your Liberty installation in the `<was_home>/wlp.bak_<timestamp>` folder. This backup folder contains the Liberty runtime at the level that it was before you started the update.

2. Use the backed-up Liberty runtime.

A copy of the Installation Manager installation and history information for this snapshot is also stored in the root of the backup in the `installed.xml` and `history.xml` files.

To determine what fixes have been installed in this snapshot, you can use the `bin/productInfo` command in the backed-up Liberty folder. See “Liberty:productInfo command” on page 1415 for more information.

You can continue using the Liberty runtime folder from its backed-up location, or you can copy or move it to a new location. If you have set the `WLP_USER_DIR` or `WLP_OUTPUT_DIR` environment variables, make sure that they point to the location of your user data and the location of output resources generated by your server respectively.

**Note:** Do not move the backed-up `wlp.bak_<timestamp>` folder back to `wlp` in case you decide to roll back to Version 8.5.0.x later.

If `WLP_USER_DIR` has not been set, the server configuration and shared resources are stored in the `usr` directory at the root of the server's runtime environment (`wlp_bak_<timestamp>/usr` for example). In this case, no action is required to use the backed-up runtime because the user data can still be found under the `usr` directory of the new location.

If the `WLP_OUTPUT_DIR` value is not set, the default location is in the server root directory (`wlp_bak_<timestamp>/usr/servers/<server_name>` for example). If this environment variable is not set, no action is required to use the backed up runtime because logs continue to appear under the `usr/servers/<server_name>/logs` directory of the new location.

For more information on these environment variables, see “Customizing the Liberty environment” on page 1565.

**Note:** If the `server.xml` file or any included XML configuration file references another resource outside the server configuration directory, ensure that these resources can be found from the new server location.

Start all Liberty servers with the `--clean` parameter as a launch option. For example:

```
server start --clean
```

You need to use the `--clean` option only once. All subsequent server starts will not require it.

If you need to continue using the backed-up Liberty in the `wlp.bak_<timestamp>` folder, you can apply fixes using the archive interim-fix service procedure documented in “Applying an interim fix to a Liberty archive installation” on page 1388.

3. Install WebSphere Application Server Liberty Network Deployment Version 8.5.5 or later.

See “Installing and uninstalling Liberty using Installation Manager” on page 1164 or “Installing and uninstalling Liberty using downloaded files and archives” on page 1371.

**Tip:** After you install WebSphere Application Server Liberty Network Deployment Version 8.5.5 or later, you can use the `ProductInfo compare` action to compare the old and new installations. This will

show any issues that were resolved in the Version 8.5.0.x level that are not resolved at the Version 8.5.5.x level. See “Liberty:productInfo command” on page 1415 for more information.

4. Start using the WebSphere Application Server Liberty Network Deployment Version 8.5.5 installation. If the WLP\_USER\_DIR and WLP\_OUTPUT\_DIR environment variables are set, then the new Liberty installation will continue using these locations to for user data, including server configurations, and to place server generated output. In this case, it is recommended that you make a backup of the directories referenced by WLP\_USER\_DIR and WLP\_OUTPUT\_DIR before beginning to use the new installation.

If the WLP\_USER\_DIR and WLP\_OUTPUT\_DIR environment variables are not set, Liberty will use folders relative to the installed runtime by default. In this case, you should copy the contents of the backed-up Liberty runtime user folder (`wlp.bak_<timestamp>/usr`) to the `usr` folder of your new installation.

For more information on these environment variables, see “Customizing the Liberty environment” on page 1565.

**Note:** If the `server.xml` file or any included XML configuration file references another resource outside the server configuration directory, ensure that these resources can be found from the new server location.

## Installing the Extended Programming Models

Distributed operating systems

8.5.5.4

Installing and updating Liberty with the Extended Programming Models differs depending on the version of WebSphere Application Server.

### About this task

The Extended Programming Models provide a rich set of programming models such as web services, JMS (including Message-driven beans), and MongoDB 2.0.

How you install the Extended Programming Models depends on your version of WebSphere Application Server:

- Up to Version 8.5.5.3: Extended Programming Models are available as the `extprogmodels` Installation Manager installable feature.
- Version 8.5.5.4 and later: Extended Programming Models are available as the `extendedPackage-1.0` Liberty Repository add-on

You can use the following options to install the Extended Programming Models when you install Liberty or to update an existing copy of Liberty to include the Extended Programming Models:

- Install or update Liberty with the Extended Programming Models using the GUI.
- Install or update Liberty with the Extended Programming Models using the command line.
- Install or update Liberty with the Extended Programming Models using response files.

**Note:** If you are installing or updating to Version 8.5.5.3 or earlier using a remote repository, such as IBM Passport Advantage or a centrally-hosted HTTP server, internet access is required to update the Extended Programming Models.

After you install Liberty Version 8.5.5.4 or later, you can later install the `extendedPackage-1.0` add-on by using the **featureManager** command. For Version 8.5.5.6 and later, you can also use the **installUtility** command to install the add-on from multiple types of repositories. For more information, see “Installing assets using the featureManager command” on page 1403 and “Installing assets using the installUtility command” on page 1393.

## Procedure

Use one of the following options to install the Extended Programming Models:

- Install or update Liberty with the Extended Programming Models using the GUI.
  - For Version 8.5.5.3 and previous versions, in the Features panel, select the **Extended Programming Models** feature.
  - For Version 8.5.5.4 and later, use the Asset Selection Wizard to install the **Extended Programming Models** addon.

For more information, see “Installing Liberty on distributed operating systems using the GUI” on page 1171.

- Install or update Liberty with the Extended Programming Models using the command line.

- V8.5.5.3 and previous versions install the `extprogmodels` feature after the product:

```
imcl install com.ibm.websphere.liberty.ND.v85,extprogmodels
-installationDirectory D:\IBM\Liberty -acceptLicense
-repositories D:\IBM\LibertyRepo
-sharedResourcesDirectory D:\IBM\IMShared
-showProgress
```

- V8.5.5.4 and later versions install the `extendedPackage-1.0` addon on the `-properties user.addon` parameter:

```
imcl install com.ibm.websphere.liberty.ND.v85
-property user.accept.license=true,user.addon=extendedPackage-1.0
-installationDirectory D:\IBM\Liberty -acceptLicense
-repositories D:\IBM\LibertyRepo
-sharedResourcesDirectory D:\IBM\IMShared
-showProgress
```

- Install or update Liberty with the Extended Programming Models using response files.

- V8.5.5.3 and previous versions install the `extprogmodels` feature on the feature attribute of the offering element:

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <variables>
    <variable name='sharedLocation' value='/opt/IBM/IMShared'/>
  </variables>
  <server>
    <repository location='http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85'/>
  </server>
  <profile id='WebSphere Liberty V8.5' installLocation='/opt/IBM/WebSphere/Liberty'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere/Liberty'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <install modify='false'>
    <!-- Install the IBM WebSphere Application Server Network Deployment 8.5.5.0 Liberty with the Extended Programming Models-->
    <offering profile='WebSphere Liberty V8.5' id='com.ibm.websphere.liberty.ND.v85' features='liberty,extprogmodels' installFixes='none'/>
  </install>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='${sharedLocation}'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
  <preference name='offering.service.repositories.areUsed' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

- V8.5.5.4 and later versions install the `extendedPackage-1.0` addon on the `user.addon` parameter under the profile element:

```

<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <variables>
    <variable name='sharedLocation' value='/opt/IBM/IMShared' />
  </variables>
  <server>
    <repository location='http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85' />
  </server>
  <profile id='WebSphere Liberty V8.5' installLocation='/opt/IBM/WebSphere/Liberty'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere/Liberty' />
    <data key='user.import.profile' value='false' />
    <data key='cic.selector.os' value='linux' />
    <data key='cic.selector.arch' value='x86_64' />
    <data key='cic.selector.ws' value='gtk' />
    <data key='cic.selector.nl' value='en' />
    <!-- Extended Programming Model add-on -->
    <data key='user.addon' value='com.ibm.websphere.appserver.extendedPackage-1.0' />
    <data key='user.accept.license' value='true' />
  </profile>
  <install modify='false'>
    <!-- IBM WebSphere Application Server Network Deployment 8.5.5.4 Liberty -->
    <offering profile='WebSphere Liberty V8.5' id='com.ibm.websphere.liberty.ND.v85' features='liberty,embeddablecontainer' installFixes='none' />
  </install>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='${sharedLocation}' />
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45' />
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
  <preference name='offering.service.repositories.areUsed' value='false' />
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
  <preference name='http.ntlm.auth.kind' value='NTLM' />
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
  <preference name='PassportAdvantageIsEnabled' value='false' />
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false' />
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true' />
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true' />
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true' />
</agent-input>

```

## Adding and removing features from Liberty on distributed operating systems

**8.5.5.0**

You can use Installation Manager to install and remove WebSphere Application Server LibertyNetwork Deployment features.

### Before you begin

Ensure that your Installation Manager preferences are pointing to the appropriate web-based or local repositories containing WebSphere Application Server Liberty Network Deployment.

### About this task

You can use the Installation Manager to install or remove features using one of the following procedures:

- Using the GUI
- Using a silent response file

You can record this response file using the GUI and Installation Manager's record mode, or you can manually create or modify a response file to suit your needs.

- Using the **imcl** command-line tool

Go to the IBM Installation Manager Information Center for more information.

### Procedure

1. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being modified.
2. Start Installation Manager.
3. Click **Modify**.
4. Select the package group to modify.

5. Click **Next**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

6. Expand IBM WebSphere Application Server Liberty Network Deployment.

7. Select the appropriate checkbox to install a feature, or clear the appropriate checkbox to remove a feature if you already have it installed.

- Embeddable EJB container and JPA client

This option installs the embeddable EJB container and JPA client.

The embeddable EJB container is a Java archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition (SE) environment. You can run enterprise beans using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.

The JPA client can be used with the embeddable EJB container to provide Java Persistence API capability in a Java SE environment.

- Extended Programming Models

The Extended Programming Models feature provides a rich set of programming models such as Web Services, JMS (including Message-Driven Beans), and Mongo 2.0.



8.5.5.4

Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` addon, or install the individual features that you need from the Liberty Repository. See the following topics for more information:

- Installing Liberty Repository assets
- Liberty features

**Note:** To install assets from the IBM WebSphere Liberty Repository, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later.

8. Click **Next**.

9. Review the summary information, and click **Modify**.

- If the modification is successful, the program displays a message indicating that installation is successful.
- If the modification is not successful, click **View Log File** to troubleshoot the problem.

10. Click **Finish**.

11. Click **File > Exit** to close Installation Manager.

## Examples

In the following examples, the optional feature offering names are enclosed in parentheses; for example: Embeddable EJB container and JPA client (`embeddablecontainer`)

- **Windows** Example of a response file that adds a feature to an installation:

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean='true' temporary='true'>
<server>
<repository location='http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85' />
</server>
<install modify='true'>
<offering id='com.ibm.websphere.liberty.ND.v85'
  profile='WebSphere Liberty V8.5'
  features='embeddablecontainer' />
</install>
<profile id='WebSphere Liberty V8.5'
  installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
</agent-input>
```

- **Windows** Example of the `imcl` command that is modified to add features to an installation:

```

imcl.exe modify com.ibm.websphere.liberty.ND.v85
-addFeatures embeddablecontainer
-repositories http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85
-installationDirectory C:\Program Files\IBM\WebSphere\Liberty
-secureStorageFile C:\credential.store -masterPasswordFile C:\master_password_file.txt

```

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

- Example of the **imcl** command that is modified to remove a feature from an installation:

```

imcl.exe modify com.ibm.websphere.liberty.ND.v85
-removeFeatures embeddablecontainer
-repositories http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85
-installationDirectory C:\Program Files\IBM\WebSphere\Liberty
-secureStorageFile C:\credential.store -masterPasswordFile C:\master_password_file.txt

```

## Uninstalling Liberty from distributed operating systems using the GUI

**8.5.5.0**

You can use the Installation Manager GUI to uninstall WebSphere Application Server Liberty Network Deployment.

### Procedure

1. Uninstall WebSphere Application Server Liberty Network Deployment.
  - a. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
  - b. Start Installation Manager.
  - c. Click **Uninstall**.
  - d. In the **Uninstall Packages** window, perform the following actions.
    - 1) Select **IBM WebSphere Application Server Liberty Network Deployment** and the appropriate version.

**Note:** If you are uninstalling the trial version of this offering, select **IBM WebSphere Application Server Liberty Network Deployment Trial** and the appropriate version. When you uninstall the IBM WebSphere Application Server Liberty Network Deployment package, you must uninstall all the packages under the same package group that are extensions to the IBM WebSphere Application Server Liberty Network Deployment package. IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty is such an extension.
    - 2) Click **Next**.
  - e. Review the summary information.
  - f. Click **Uninstall**.
    - If the uninstallation is successful, the program displays a message that indicates success.
    - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
  - g. Click **Finish**.
  - h. Click **File > Exit** to close Installation Manager.
2. Optional: Uninstall IBM Installation Manager.

**Important:** Before you can uninstall IBM Installation Manager, you must uninstall all of the packages that were installed by Installation Manager.

Read the IBM Installation Manager Information Center for information about performing this procedure.

## Uninstalling Liberty from distributed operating systems using the command line

8.5.5.0

You can uninstall WebSphere Application Server Liberty Network Deployment using the Installation Manager command line.

### Procedure

1. Log on to your system.
2. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
3. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
4. Use the `imcl` command to uninstall the offering.

Windows

```
imcl.exe uninstall com.ibm.websphere.liberty.ND.v85 -installationDirectory installation_directory
```

AIX

HP-UX

Linux

Solaris

```
./imcl uninstall com.ibm.websphere.liberty.ND.v85 -installationDirectory installation_directory
```

### Tips:

- Use the `imcl modify` command to add or remove features.
- When you uninstall the IBM WebSphere Application Server Liberty Network Deployment package, you must uninstall all the packages under the same package group that are extensions to the IBM WebSphere Application Server Liberty Network Deployment package. IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty is such an extension.

Go to the IBM Installation Manager Information Center for more information.

5. Optional: Uninstall IBM Installation Manager.

**Important:** Before you can uninstall IBM Installation Manager, you must uninstall all of the packages that were installed by Installation Manager.

Read the IBM Installation Manager Information Center for information about using the uninstall script to perform this procedure.

## Uninstalling Liberty from distributed operating systems by using response files

8.5.5.0

You can uninstall WebSphere Application Server Liberty Network Deployment by using Installation Manager response files.

### Before you begin

**Optional:** Perform or record the installation of Installation Manager and installation of the product to a temporary installation registry on one of your systems so that you can use this temporary registry to record the uninstall without using the standard registry where Installation Manager is installed.

### About this task

Using Installation Manager, you can work with response files to uninstall the product in various ways. You can record a response file by using the GUI as described in the following procedure. Or, you can generate a new response file by hand or by taking an example and modifying it.

## Procedure

1. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
2. Optional: **Record a response file to uninstall the product:** On one of your systems, perform the following actions to record a response file that uninstalls the product:
  - a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.
  - b. Start Installation Manager from the command line by using the **-record** option.

For example:

- **Windows Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"  
-record C:\temp\uninstall_response_file.xml
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry  
-record /var/temp/uninstall_response_file.xml
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry  
-record user_home/var/temp/uninstall_response_file.xml
```

**Tip:** If you choose to use the **-skipInstall** parameter with a temporary installation registry created as described in *Before you begin*, Installation Manager uses the temporary installation registry while recording the response file. It is important to note that when the **-skipInstall** parameter is specified, no product packages are installed or uninstalled. All of the actions that you perform in Installation Manager update the installation data that is stored in the specified temporary registry. After the response file is generated, it can be used to uninstall the product, removing the product files and updating the standard installation registry.

Do not use the **-skipInstall** operation on the actual agent data location that is used by Installation Manager. This operation is unsupported. Use a clean writable location, and reuse that location for future recording sessions.

For more information, read the IBM Installation Manager Information Center.

- c. Click **Uninstall**.
  - d. In the **Uninstall Packages** window, perform the following actions.
    - 1) Select **IBM WebSphere Application Server Liberty Network Deployment** and the appropriate version.  
  
**Note:** If you are uninstalling the trial version of this offering, select **IBM WebSphere Application Server Liberty Network Deployment Trial** and the appropriate version.
    - 2) Click **Next**.
  - e. Review the summary information.
  - f. Click **Uninstall**.
    - If the uninstallation is successful, the program displays a message that indicates success.
    - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
  - g. Click **Finish**.
  - h. Click **File > Exit** to close Installation Manager.
3. **Use the response file to uninstall the product:** From a command line on each of the systems from which you want to uninstall the product, change to the eclipse/tools sub-directory in the directory where you installed Installation Manager and use the response file that you created to uninstall the product.

For example:

- **Windows Administrator or non-administrator:**

```
imcl.exe
input C:\temp\uninstall_response_file.xml
-log C:\temp\uninstall_log.xml
```

- AIX HP-UX Linux Solaris **Administrator:**

```
./imcl
input /var/temp/uninstall_response_file.xml
-log /var/temp/uninstall_log.xml
```

- AIX HP-UX Linux Solaris **Non-administrator:**

```
./imcl
input user_home/var/temp/uninstall_response_file.xml
-log user_home/var/temp/uninstall_log.xml
```

Go to the IBM Installation Manager Information Center for more information.

#### 4. Optional: List all installed packages to verify the uninstallation.

AIX HP-UX Linux Solaris

```
./imcl listInstalledPackages
```

Windows

```
imcl listInstalledPackages
```

#### 5. Optional: Uninstall IBM Installation Manager.

**Important:** Before you can uninstall IBM Installation Manager, you must uninstall all of the packages that were installed by Installation Manager.

Read the IBM Installation Manager Information Center for information about using the uninstall script to perform this procedure.

Windows

### Example

The following is an example of a response file for uninstalling the product.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean='true' temporary='true'>
<uninstall modify='false'>
<offering id='com.ibm.websphere.liberty.ND.v85'
  profile='WebSphere Liberty V8.5' />
</uninstall>
<profile id='WebSphere Liberty V8.5'
  installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
</agent-input>
```

**Tip:** When you uninstall the IBM WebSphere Application Server Liberty Network Deployment package, you must uninstall all the packages under the same package group that are extensions to the IBM WebSphere Application Server Liberty Network Deployment package. IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty is such an extension. To uninstall the entire package group, remove the id attribute in the <offering ../> stanza (id='com.ibm.websphere.liberty.ND.v85' in the previous example) from the response file. Installation Manager then uninstalls all of the packages under the package group.

## Installing and uninstalling Liberty interim fixes and fix packs on distributed operating systems

**8.5.5.0**

Interim fixes provide corrective service for specific known problems. Fix packs contain bundled service to bring WebSphere Application Server Liberty Network Deployment up to a new level. You can use IBM Installation Manager to update the offering with the interim fixes and fix packs that are available for your service level of WebSphere Application Server Liberty Network Deployment.

## Before you begin

Contact the IBM Software Support Center for information about updates for WebSphere Application Server Liberty Network Deployment. The most current information is available from the IBM Software Support Center and Fix Central.

IBM Installation Manager is used to apply and remove maintenance.

**Important:** Installation Manager can install any fix-pack level of the product directly without installing the intermediate fix packs; in fact, Installation Manager installs the latest level by default. For example, you can skip fix-pack levels and go from Version 8.5.5.1 directly to Version 8.5.5.5. Keep in mind, however, that later you can not roll back to any level that was skipped. If you directly install to Version 8.5.5.5, for example, you cannot roll back to Version 8.5.5.4. If you skip from Version 8.5.5.1 to Version 8.5.5.5, you can only roll back to Version 8.5.5.1. You should plan your installations accordingly.

- | **New:** Fix pack 16.0.0.2 is the next fix pack after 8.5.5.9. You can continue to use the same Version 8.5
- | Installation Manager repositories and offering IDs to install or update to 16.0.0.2, or you can use the new
- | versionless repositories and offerings. For more information about fix pack 16.0.0.2, see What is new in
- | Liberty in the new location of the latest Liberty documentation.

**Note:** In WebSphere Application Server Version 8.5.5.0, Liberty was promoted from a feature to an independently installable offering. After updating to WebSphere Application Server Liberty Network Deployment Version 8.5.5.x from Version 8.5.0.x, you can roll back to the Version 8.5.0.x Liberty feature level that you were at before updating. If you previously had a combined full-profile and Liberty installation, the Liberty feature will be reinstalled to the wlp folder when you roll back. Any user data and server configurations will not be restored. If necessary, you can copy them from the backed-up location into the new wlp/usr folder after rollback. If any wlp.bak\_<timestamp> directories are present in your installation image, they will not be affected by the rollback. If you update and roll back multiple times between Version 8.5.0.x and Version 8.5.5.x levels, therefore, you will have multiple wlp.bak\_<timestamp> folders in your installation image. These can always be deleted, copied, or moved without negative impact to your installation.

## About this task

**Tip:** You can use the IBM Packaging Utility to generate a new local or web-based repository that contains all of the fixes that you want to install and then use Installation Manager to update WebSphere Application Server Liberty Network Deployment with all of the interim fixes as a group. For information on using the Packaging Utility, see the IBM Installation Manager Information Center.

## Procedure

- “Installing Liberty interim fixes on distributed operating systems using the GUI” on page 1193
- “Installing Liberty interim fixes on distributed operating systems using the command line” on page 1195
- “Uninstalling Liberty interim fixes from distributed operating systems using the GUI” on page 1197
- “Uninstalling Liberty interim fixes from distributed operating systems using the command line” on page 1198
- “Installing Liberty fix packs on distributed operating systems using the GUI” on page 1198
- “Installing Liberty fix packs on distributed operating systems using the command line” on page 1200
- “Installing Liberty fix packs on distributed operating systems using response files” on page 1204
- “Uninstalling Liberty fix packs from distributed operating systems using the GUI” on page 1209
- “Uninstalling Liberty fix packs from distributed operating systems using the command line” on page 1210

- “Uninstalling Liberty fix packs from distributed operating systems by using response files” on page 1212
- AIX HP-UX Linux Solaris Optional: After the fix pack is installed or removed, reapply any ownership and permissions changes that were made after the offering was originally installed.

## Installing Liberty interim fixes on distributed operating systems using the GUI: 8.5.5.0

You can use the IBM Installation Manager graphical user interface (GUI) to update the offering with the interim fixes that are available for your service level of WebSphere Application Server Liberty Network Deployment.

### Before you begin

Contact the IBM Software Support Center for information about updates for WebSphere Application Server Liberty Network Deployment. The most current information is available from the IBM Software Support Center and Fix Central.

Make sure that the web-based or local service repository location is listed and checked or that the **Search service repositories during installation and updates** option is selected on the Repositories panel in your Installation Manager preferences. For more information on using service repositories with Installation Manager, read the IBM Installation Manager Information Center.

### Procedure

1. For a list of fixes that are available for WebSphere Application Server Liberty Network Deployment and specific information about each fix, perform the following actions.
  - a. Go to Fix Central.
  - b. Select **WebSphere** as the product group.
  - c. Select **WebSphere Application Server Liberty Network Deployment** as the product.
  - d. Select the installed version.
  - e. Select your operating system as the platform, and click **Continue**.
  - f. Select **Browse for fixes**, and click **Continue**.
  - g. Click **More Information** under each fix to view information about the fix.
  - h. **Recommendation:** Make a list of the names of the fixes that you would like to install.
2. Update WebSphere Application Server Liberty Network Deployment with the fixes using one of the following procedures.
  - Access the live service repository that contains the fixes, and use web-based updating. Use Installation Manager on your local system to update WebSphere Application Server Liberty Network Deployment with the interim fixes from the live web-based service repositories.
    - For the live service repositories, use the same URLs as those used for the generally available product-offering repositories during installation. These URLs are listed in Online product repositories for WebSphere Application Server offerings.
    - These locations do not contain web pages that you can access using a web browser. They are remote web-based repository locations that you specify for Installation Manager so that it can maintain the offering.

To install a fix from a service repository, perform the following actions:

  - a. Log on to your system.
  - b. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being updated.
  - c. Start Installation Manager.
  - d. Click **Update**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you use to access protected IBM software websites.

- e. Select the package group to update with the fix.

**Tip:** If the **Search service repositories during installation and updates** option is selected on the Installation Manager Repository preference page and you are connected to the Internet, you can click **Check for Other Versions and Extensions** to search for updates in the default update repositories for the selected packages. In this case, you do not need to add the specific service-repository URL to the Installation Manager Repository preference page.

- f. Click **Next**.

- g. Select the fixes to install, and click **Next**.

Any recommended fixes are selected by default.

If there are recommended fixes, you can select the option to show only recommended fixes and hide non-recommended fixes.

- h. Review the summary information, and click **Update**.

- i. Click **Finish**.

- j. Click **File > Exit** to close Installation Manager.

- Download the files that contain the fixes from Fix Central, and use local updating.

You can download compressed files that contain the fixes from Fix Central. Each compressed fix file contains an Installation Manager repository for the fix and usually has a .zip extension. After downloading the fix files, you can use one of the following procedures to update WebSphere Application Server Liberty Network Deployment:

- Use Installation Manager to update WebSphere Application Server Liberty Network Deployment with the fixes.
- Use the IBM Packaging Utility to generate a new repository that contains all of the fix files that you downloaded, then use Installation Manager to update WebSphere Application Server Liberty Network Deployment with all of the fixes as a group. For information on using the Packaging Utility, see the IBM Installation Manager Information Center.

- a. To download the fixes, perform the following actions:

- 1) Go to Fix Central.
- 2) Select **WebSphere** as the product group.
- 3) Select **WebSphere Application Server Liberty Network Deployment** as the product.
- 4) Select the installed version.
- 5) Select your operating system as the platform, and click **Continue**.
- 6) Select **Browse for fixes**, and click **Continue**.
- 7) Select the fixes that you want to download, and click **Continue**.
- 8) Select your download options, and click **Continue**.
- 9) Click **I agree** to agree to the terms and conditions.
- 10) Click **Download now** to download the fixes.

- b. To install a fix from a downloaded compressed file, perform the following actions:

- 1) Log on to your system.
- 2) Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being updated.
- 3) Start Installation Manager.
- 4) Add the location of the fix file that you downloaded to your Installation Manager preferences.
- 5) Click **Update**.
- 6) Select the package group to update with the fix, and click **Next**.

- 7) Select the fixes to install, and click **Next**.  
Any recommended fixes are selected by default.  
If there are recommended fixes, you can select the option to show only recommended fixes and hide non-recommended fixes.
- 8) Review the summary information, and click **Update**.
- 9) Click **Finish**.
- 10) Click **File > Exit** to close Installation Manager.

### Installing Liberty interim fixes on distributed operating systems using the command line:

**8.5.5.0**

You can use the IBM Installation Manager command line to update the offering with the interim fixes that are available for your service level of WebSphere Application Server Liberty Network Deployment.

#### Before you begin

Contact the IBM Software Support Center for information about updates for WebSphere Application Server Liberty Network Deployment. The most current information is available from the IBM Software Support Center and Fix Central.

IBM Installation Manager is used to apply maintenance to WebSphere Application Server Liberty Network Deployment.

#### Procedure

1. For a list of interim fixes and fix packs that are available for WebSphere Application Server LibertyNetwork Deployment and specific information about each fix, perform the following actions.
  - a. Go to Fix Central.
  - b. Select **WebSphere** as the product group.
  - c. Select **WebSphere Application Server Liberty Network Deployment** as the product.
  - d. Select the version of the offering to be updated.
  - e. Select your operating system as the platform, and click **Continue**.
  - f. Select **Browse for fixes**, and click **Continue**.
  - g. Click **More Information** under each fix to view information about the fix.
  - h. **Recommendation:** Make a list of the names of the fixes that you would like to install.
2. Update WebSphere Application Server Liberty Network Deployment with the interim fixes using one of the following procedures.
  - **Access the live service repository that contains the interim fixes, and use web-based updating.**  
Use Installation Manager on your local system to update WebSphere Application Server LibertyNetwork Deployment with the interim fixes from the live web-based service repositories.
    - For the live service repositories, use the same URLs as those used for the generally available product-offering repositories during installation. These URLs are listed in Online product repositories for WebSphere Application Server offerings.
    - These locations do not contain web pages that you can access using a web browser. They are remote web-based repository locations that you specify for Installation Manager so that it can maintain the offering.

To install an interim fix from a service repository, perform the following actions:

    - a. Log on to your system.
    - b. If you do not already have Installation Manager credential-storage and master-password files containing your IBM software user ID and password, create files that will allow you to access the repository.

**Note:** These are the credentials that you use to access protected IBM software websites. For information on creating credential-storage and master-password files for Installation Manager, read the IBM Installation Manager Information Center.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

- c. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being updated.
- d. Change to the `Installation_Manager_binaries/eclipse/tools` directory, where `Installation_Manager_binaries` is the installation root directory for the Installation Manager.
- e. Install the interim fix.

```
AIX      HP-UX    Linux   Solaris

./imcl install fix_name
  -installationDirectory offering_installation_location
  -repositories repository_URL
  -secureStorageFile storage_file -masterPasswordFile master_password_file
```

```
Windows

imcl.exe install fix_name
  -installationDirectory offering_installation_location
  -repositories repository_URL
  -secureStorageFile storage_file -masterPasswordFile master_password_file
```

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the `-keyring` and `-password` options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the `-keyring` and `-password` options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

- f. **Optional:** List all installed packages to verify the installation:

```
AIX      HP-UX    Linux   Solaris

./imcl listInstalledPackages -long

Windows

imcl.exe listInstalledPackages -long
```

- **Download the files that contain the interim fixes from Fix Central, and use local updating.**

You can download compressed files that contain the interim fixes from Fix Central. Each compressed fix file contains an Installation Manager repository for the interim fix and usually has a `.zip` extension. After downloading the fix files, you can use one of the following procedures to update WebSphere Application Server Liberty Network Deployment:

- Use Installation Manager to update WebSphere Application Server Liberty Network Deployment with the interim fixes.
  - Use the IBM Packaging Utility to generate a new repository that contains all of the fix files that you downloaded, then use Installation Manager to update WebSphere Application Server Liberty Network Deployment with all of the interim fixes as a group. For information on using the Packaging Utility, see the IBM Installation Manager Information Center.
- a. To download the interim fixes, perform the following actions:
    - 1) Go to Fix Central.
    - 2) Select **WebSphere** as the product group.

- 3) Select **WebSphere Application Server Liberty Network Deployment** as the product.
  - 4) Select the version of the offering to be updated.
  - 5) Select your operating system as the platform, and click **Continue**.
  - 6) Select **Browse for fixes**, and click **Continue**.
  - 7) Select the interim fixes that you want to download, and click **Continue**.
  - 8) Select your download options, and click **Continue**.
  - 9) Click **I agree** to agree to the terms and conditions.
  - 10) Click **Download now** to download the interim fixes.
- b. To install an interim fix from a downloaded compressed file, perform the following actions:
- 1) Log on to your system.
  - 2) Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being updated.
  - 3) Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager.
  - 4) Install the interim fix.

AIX

HP-UX

Linux

Solaris

```
./imcl install fix_name
-installationDirectory offering_installation_location
-repositories compressed_file
```

Windows

```
imcl.exe install fix_name
-installationDirectory offering_installation_location
-repositories compressed_file
```

- 5) **Optional:** List all installed packages to verify the installation:

AIX

HP-UX

Linux

Solaris

```
./imcl listInstalledPackages -long
```

Windows

```
imcl.exe listInstalledPackages -long
```

## Uninstalling Liberty interim fixes from distributed operating systems using the GUI: 8.5.5.0

You can use the IBM Installation Manager graphical user interface (GUI) to remove interim fixes from WebSphere Application Server Liberty Network Deployment.

### Procedure

1. Log on to your system.
2. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being updated.
3. Start Installation Manager.
4. Click **Uninstall**.
5. Select the interim fixes to uninstall.
6. Click **Next**.
7. Review the summary information, and click **Uninstall**.
  - If the uninstallation is successful, the program displays a message indicating that the uninstallation is successful.
  - If the uninstallation is not successful, click **View Log File** to troubleshoot the problem.
8. Click **Finish**.

9. Click **File > Exit** to close Installation Manager.

### Uninstalling Liberty interim fixes from distributed operating systems using the command line:

**8.5.5.0**

You can use the IBM Installation Manager command-line function to remove interim fixes from WebSphere Application Server Liberty Network Deployment.

#### Procedure

1. Log on to your system.
2. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being updated.
3. Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager.
4. Uninstall the interim fix:

**AIX**

**HP-UX**

**Linux**

**Solaris**

```
./imcl uninstall interim_fix_name  
-installationDirectory offering_installation_location
```

**Windows**

```
imcl.exe uninstall interim_fix_name  
-installationDirectory offering_installation_location
```

### Installing Liberty fix packs on distributed operating systems using the GUI: **8.5.5.0**

You can update WebSphere Application Server Liberty Network Deployment to a later version using the Installation Manager GUI.

#### Before you begin

Contact the IBM Software Support Center for information about updates for WebSphere Application Server Liberty Network Deployment. The most current information is available from the IBM Software Support Center and Fix Central.

**8.5.5.4**

To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

Make sure that the web-based or local service repository location is listed and checked or that the **Search service repositories during installation and updates** option is selected on the Repositories panel in your Installation Manager preferences. For more information on using service repositories with Installation Manager, read the IBM Installation Manager Information Center.



**8.5.5.6**

If you want to install Liberty assets from local directory-based repositories or an instance of the Liberty Asset Repository Service, configure the repositories. For more information about the Liberty asset repositories, see “Installing assets using Installation Manager” on page 1411.

#### Procedure

1. Log on to your system.
2. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
3. Start Installation Manager.
4. Click **Update**.

**Note:** If prompted to authenticate, specify the IBM ID and password that you use to access protected IBM software websites.

5. Select the package group to update. If you select **Update all**, Installation Manager searches all of the added and predefined repositories for recommended updates to all of the package groups that it has installed.
  - Use this feature only if you have full control over which fixes are contained in the targeted repositories.
    - If you create and point to a set of custom repositories that include only the specific recommended fixes that you want to install, you should be able to use this feature confidently.
    - If you enable searching service repositories or install fixes directly from other live web-based repositories, you might not want to select this option so that you can select only the fixes that you want to install for each offering on subsequent panels.
  - If you select **Update all**, Installation Manager will install only the recommended updates to all of the package groups; it will not allow you to select non-recommended fixes for installation. If you want to install non-recommended fixes, perform the following actions:
    - a. On this panel, clear the **Update all** check box and select an offering to update.
    - b. On the next panel, clear the option to show only recommended fixes and then select the fixes that you want to install.
  - **8.5.5.4** The **Update all** option might generate a warning message if you complete the following steps:
    - a. Install WebSphere Application Server Liberty v8.5.5.3 with the Extended Programming Model.
    - b. Install WebSphere Application Server Network Deployment Liberty v8.5.5.3 with the Extended Programming Model.
    - c. Select **Update all**. Click **Next**.
    - d. You might receive an Update Validation Warning message with multiple messages. Click **OK**. Click **Next**.
    - e. You might receive the Extended Programming Model Warning message panel.
    - f. Click **Back** to the Update Package panel. Click **Next**.
    - g. You might again receive an Update Validation Warning message with multiple messages.
    - h. From the Extended Programming Model Warning message panel, click **Next**. In the Offering License panel, find the following error:

An error has occurred. See error log for more details. Bundle "reference:file:/C:/ProgramData/IBM/InstallationTo fix this problem, complete the following steps:
    - a. Click **Cancel**.
    - b. Select **Update all**.
    - c. Do not click **Back**. This action causes the error that uninstalls the license.
6. Click **Next**.
7. Select the version to which you want to update under **IBM WebSphere Application Server Liberty Network Deployment**.
8. Select any fixes that you want to install. Any recommended fixes are selected by default. If there are recommended fixes, you can select the option to show only recommended fixes and hide non-recommended fixes.
9. Click **Next**.
10. Accept the terms in the license agreements, and click **Next**.
11. Select the optional features that you want in your updated installation.

**8.5.5.4**

Beginning with Version 8.5.5.4, the Extended Programming Model is available from the Liberty Repository. This asset provides a rich set of programming models such as Web Services, JMS (including Message-Driven Beans), and MongoDB 2.0. To install this asset, use the Asset Selection Wizard as described in the next step.

12.  **8.5.5.2** Optional: Install additional Liberty Repository assets. If you do not want to select any additional assets, you can skip this step. To install Liberty Repository assets, you must have IBM Installation Manager Version 1.6.2 or later. To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.
  - a. Select whether you want to install assets from the Liberty Repository, and click **Next**. To install assets from the IBM WebSphere Liberty Repository, you must have access to the internet.
 

**8.5.5.6** If you choose not to connect to the IBM WebSphere Liberty Repository, you can still install assets from configured directory-based repositories or an instance of the Liberty Asset Repository Service. For more information, see “Installing assets using Installation Manager” on page 1411.
  - b. **8.5.5.4** Click **Launch Asset Selection Wizard**.
  - c. You can perform a case-insensitive search for assets by display name or description. If you search with the **Keyword** field empty, then the search displays all applicable assets.
 

**8.5.5.5** With Version 8.5.5.5 and later, you can also search for assets by short name.
  - d. Select each asset that you want to install, then click **Next**.
  - e. Accept the license agreement and click **Finish**.
13. Review the summary information, and click **Update**.
  - If the installation is successful, the program displays a message indicating that installation is successful.
  - If the installation is not successful, click **View Log File** to troubleshoot the problem.
14. Click **Finish**.
15. Click **File > Exit** to close Installation Manager.

### Installing Liberty fix packs on distributed operating systems using the command line: **8.5.5.0**

You can use the IBM Installation Manager command line to update the product with the fix packs that are available for WebSphere Application Server LibertyNetwork Deployment.

#### Before you begin

Contact the IBM Software Support Center for information about updates for WebSphere Application Server Liberty Network Deployment. The most current information is available from the IBM Software Support Center and Fix Central.

**8.5.5.6**

If you want to install Liberty assets from local directory-based repositories or an instance of the Liberty Asset Repository Service, configure the repositories. For more information about the Liberty asset repositories, see “Installing assets using Installation Manager” on page 1411.

**Tip:** As an alternative to the procedure that is described in this article, Installation Manager allows you to use the **updateAll** command in a response file or on the command line to search for and update all installed packages. Use this command only if you have full control over which fixes are contained in the targeted repositories. You can create and point to a set of custom repositories that include only the specific fixes that you want to install. If you enable searching service repositories or install fixes directly from other live web-based repositories, then you might not want to select this option so that you can select only the fixes that you want to install using the **-installFixes** option with the **install** command on the command line or the **installFixes** attribute in a response file.

## About this task

**8.5.5.4** To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

### Procedure

1. For a list of interim fixes and fix packs that are available for WebSphere Application Server LibertyNetwork Deployment and specific information about each fix, perform the following actions.
  - a. Go to Fix Central.
  - b. Select **WebSphere** as the product group.
  - c. Select **WebSphere Application Server** as the product.
  - d. Select the installed version.
  - e. Select your operating system as the platform, and click **Continue**.
  - f. Select **Browse for fixes**, and click **Continue**.
  - g. Click **More Information** under each fix to view information about the fix.
  - h. **Recommendation:** Make a note of the name of the fix pack that you would like to install.
2. Update WebSphere Application Server Liberty Network Deployment with the fix pack using one of the following procedures.
  - Access the live service repository that contains the fix pack, and use web-based updating. Use Installation Manager on your local system to update WebSphere Application Server Liberty Network Deployment with the interim fixes from the live web-based service repositories.
    - For the live service repositories, use the same URLs as those used for the generally available product-offering repositories during installation. These URLs are based on the following pattern:  
`http://www.ibm.com/software/repositorymanager/offering_ID`

where *offering\_ID* is the offering ID that you can find in WebSphere Application Server product offerings for supported operating systems.

- These locations do not contain web pages that you can access using a web browser. They are remote web-based repository locations that you specify for Installation Manager so that it can maintain the product.

To install a fix pack from a service repository, perform the following actions:

- a. Log on to your system.
- b. Create Installation Manager credential-storage and master-password files that contain your IBM software user ID and password. These files enable you to access the repository and protected IBM software websites.

When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

**Note:** For Installation Manager Version 1.6.2 and later, use the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file. In previous versions, the `-keyring` and `-password` options are used to access credentials in a keyring file. These options are deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures.

- For more information on using the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation.
  - For more information on using the `-keyring` and `-password` options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.
- c. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being updated.

- d. Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager.
- e. Install the fix pack.

**AIX** **HP-UX** **Linux** **Solaris**

```
./imcl install offering_ID_offering_version,optional_feature_ID
-repositories source_repository
-installationDirectory offering_installation_location
-secureStorageFile storage_file -masterPasswordFile master_password_file
-acceptLicense
```

**Windows**

```
imcl.exe install offering_ID_offering_version,optional_feature_ID
-repositories source_repository
-installationDirectory offering_installation_location
-secureStorageFile storage_file -masterPasswordFile master_password_file
-acceptLicense
```

where *offering\_ID* is the offering ID that is listed in WebSphere Application Server product offerings for supported operating systems.

#### Tips:

- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.5.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the `-installFixes` option defaults to all.
  - If the offering version is specified, the `-installFixes` option defaults to none.
- You can add a list of features that are separated by commas.
-  **8.5.5.2** You can specify additional features to install from the Liberty Repository. For a list of Liberty Repository assets, see the downloads page on WASdev.net.

**Note:** To install Liberty Repository assets, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later.

If you want to install additional features, specify the following properties in the command line. Note that the feature short names, such as *FeatureA*, are separated by double commas:

```
-properties user.feature=FeatureA,,FeatureB,,FeatureC,user.accept.license=true
```

For Version 8.5.5.5 and later, `user.accept.license=true` is not required.

-  **8.5.5.4** Beginning with Version 8.5.5.4, the Extended Programming Models are available to download from the Liberty Repository as the `extendedPackage-1.0` addon. This addon provides a rich set of programming models such as Web Services, JMS (including Message-Driven Beans), and MongoDB 2.0. To install the addon, specify the `extendedPackage-1.0` addon on the **user.addon** option of the **-properties** parameter:

```

imcl install com.ibm.websphere.liberty.ND.v85
-properties user.acceptLicense=true,user.addon=extendedPackage-1.0
-installationDirectory D:\IBM\Liberty -acceptLicense
-repositories D:\IBM\LibertyRepo
-sharedResourcesDirectory D:\IBM\IMShared
-showProgress

```



8.5.5.6

You can also install assets from instances of the Liberty Asset Repository Service or local directory-based repositories. For more information about these asset repositories, see “Installing assets using Installation Manager” on page 1411. Add the repository on the **-repositories** parameter. The repositories are accessed in the order that they are specified. By default, the Liberty Repository is the last of the repositories that are accessed during installation. To disable access to the Liberty Repository, on the **-properties** parameter, set the **user.useLibertyRepository** option to false.

8.5.5.8

```

imcl install com.ibm.websphere.liberty.ND.v85
-properties user.useLibertyRepository=false,user.addon=extendedPackage-1.0,user.feature=portlet-2.0
-installationDirectory D:\IBM\Liberty -acceptLicense
-repositories D:\IBM\LibertyProductRepo,https://your_onprem_asset_repo_url,D:\IBM\LocalAssetRepo,D:\IBM\LocalAssetRepo2.zip
-sharedResourcesDirectory D:\IBM\IMShared
-showProgress

```

To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.

**Note:** If you do not have the Extended Programming Model installed prior to updating to Version 8.5.5.4, you might encounter the following error during the update:

8.5.5.4

```

java.io.IOException: Too many open files
at java.io.File.createNewFile(File.java:894)

```

To resolve this problem, increase the number of files using the **ulimit** command; for example:

```
ulimit -n 8192
```

- f. List all installed packages to verify the installation:

AIX

HP-UX

Linux

Solaris

```
./imcl listInstalledPackages -long
```

Windows

```
imcl.exe listInstalledPackages -long
```

- Download the file that contains the fix pack from Fix Central, and use local updating. You can download a compressed file that contains the fix pack from Fix Central. Each compressed fix-pack file contains an Installation Manager repository for the fix pack and usually has a .zip extension. After downloading and extracting the fix-pack file, use Installation Manager to update WebSphere Application Server Liberty Network Deployment with the fix pack.
  - a. To download the fix pack, perform the following actions:
    - 1) Go to Fix Central.
    - 2) Select **WebSphere** as the product group.
    - 3) Select **WebSphere Application Server** as the product.
    - 4) Select the installed version.
    - 5) Select your operating system as the platform, and click **Continue**.
    - 6) Select **Browse for fixes**, and click **Continue**.
    - 7) Select the fix pack that you want to download, and click **Continue**.
    - 8) Select your download options, and click **Continue**.
    - 9) Click **I agree** to agree to the terms and conditions.
    - 10) Click **Download now** to download the fix pack.
    - 11) Transfer the compressed file in binary format to the system on which it is installed.
    - 12) Extract the compressed repository files to a directory on your system.
  - b. To install a fix pack from a downloaded file, perform the following actions:
    - 1) Log on to your system.

- 2) Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being updated.
- 3) Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager.
- 4) Install the fix pack.

AIX

HP-UX

Linux

Solaris

```
./imcl install offering_ID offering_version,optional_feature_ID
-installationDirectory offering_installation_location
-repositories location_of_expanded_files
-acceptLicense
```

Windows

```
imcl.exe install offering_ID offering_version,optional_feature_ID
-installationDirectory offering_installation_location
-repositories location_of_expanded_files
-acceptLicense
```

#### Tips:

- The *offering\_ID* is the offering ID that is listed in WebSphere Application Server product offerings for supported operating systems.
- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.5.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the *-installFixes* argument to indicate which interim fixes you want installed with the offering.
    - If the offering version is **not** specified, the *-installFixes* option defaults to all.
    - If the offering version is specified, the *-installFixes* option defaults to none.
  - You can add a list of features that are separated by commas.
- 5) **Optional:** List all installed packages to verify the installation:

AIX

HP-UX

Linux

Solaris

```
./imcl listInstalledPackages -long
```

Windows

```
imcl.exe listInstalledPackages -long
```

### Installing Liberty fix packs on distributed operating systems using response files: **8.5.5.0**

You can update WebSphere Application Server Liberty Network Deployment to a later version using Installation Manager response files.

#### About this task

**8.5.5.4** To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.



If you want to install Liberty assets from local directory-based repositories or an instance of the Liberty Asset Repository Service, configure the repositories. For more information about the Liberty asset repositories, see “Installing assets using Installation Manager” on page 1411.

**Tip:** As an alternative to the procedure that is described in this topic, use the Installation Manager **updateAll** command in a response file or on the command line to search for and update all installed packages. Use this command only if you have full control over which fixes are contained in the targeted repositories. Create and point to a set of custom repositories that include only the specific fixes that you want to install. If you enable searching service repositories or if you install fixes directly from other live web-based repositories, then you might not want to select this option so that you can select only the fixes that you want to install using the **-installFixes** option with the **install** command on the command line or the **installFixes** attribute in a response file.

### Procedure

1. To obtain a list of interim fixes and fix packs that are available for WebSphere Application Server LibertyNetwork Deployment installation and specific information about each fix, perform the following actions.
  - a. Go to Fix Central.
  - b. Select **WebSphere** as the product group.
  - c. Select **WebSphere Application Server** as the product.
  - d. Select the installed version.
  - e. Select your operating system as the platform, and click **Continue**.
  - f. Select **Browse for fixes**, and click **Continue**.
  - g. Click **More Information** under each fix to view information about the fix.
  - h. Note of the name of the fix pack that you would like to install.
2. Update WebSphere Application Server Liberty Network Deployment with the fix pack using one of the following procedures.

- Access the live service repository that contains the fix pack, and use web-based updating.

Use Installation Manager on your local system to update WebSphere Application Server Liberty Network Deployment with the interim fixes from the live web-based service repositories.

- For the live service repositories, use the same URLs as those used for the generally available product-offering repositories during installation. These URLs are based on the following pattern:  
`http://www.ibm.com/software/repositorymanager/offering_ID`

where *offering\_ID* is the offering ID that you can find in WebSphere Application Server product offerings for supported operating systems.

- These locations do not contain web pages that you can access using a web browser. They are remote web-based repository locations that you specify for Installation Manager so that it can maintain the product.

Perform the following actions:

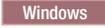
- a. Log on to your system.
- b. Create files that enable you to access the repository. Installation Manager credential-storage and master-password files contain your IBM software user ID and password and enable you to access protected IBM software websites. When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the **imutilsc** command is unable to find the URL that is specified.

**Note:** For Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In previous versions of Installation Manager, the **-keyring** and **-password** options are used to access

credentials in a keyring file. These options are deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures.

- For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation.
- For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.
- c. Stop all servers and applications on the WebSphere Application Server installation that is being updated.
- d. Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager.
- e. Install the fix pack using a response file.

For example:

-  Administrator or non-administrator:

```
imcl.exe -acceptLicense
input C:\temp\update_response_file.xml
-log C:\temp\update_log.xml
-secureStorageFile C:\IM\credential.store -masterPasswordFile C:\IM\master_password_file.txt
```

-     Administrator:

```
./imcl -acceptLicense
input /var/temp/update_response_file.xml
-log /var/temp/update_log.xml
-secureStorageFile /var/IM/credential.store -masterPasswordFile /var/IM/master_password_file.txt
```

-     Non-administrator:

```
./imcl -acceptLicense
input user_home/var/temp/update_response_file.xml
-log user_home/var/temp/update_log.xml
-secureStorageFile user_home/var/IM/credential.store -masterPasswordFile user_home/var/IM/master_password_file.txt
```

- Download the file that contains the fix pack from Fix Central, and use local updating.

You can download a compressed file that contains the fix pack from Fix Central. Each compressed fix-pack file contains an Installation Manager repository for the fix pack and usually has a .zip extension. After downloading and extracting the fix-pack file, use Installation Manager to update WebSphere Application Server Liberty with the fix pack.

- a. To download the fix pack, perform the following actions:

- 1) Go to Fix Central.
- 2) Select **WebSphere** as the product group.
- 3) Select **WebSphere Application Server** as the product.
- 4) Select the installed version.
- 5) Select your operating system as the platform, and click **Continue**.
- 6) Select **Browse for fixes**, and click **Continue**.
- 7) Select the fix pack that you want to download, and click **Continue**.
- 8) Select your download options, and click **Continue**.
- 9) Click **I agree** to agree to the terms and conditions.
- 10) Click **Download now** to download the fix pack.
- 11) Transfer the compressed file in binary format to the system on which it will be installed.
- 12) Extract the compressed repository files to a directory on your system.

- b. Perform the following actions:

- 1) Log on to your system.
- 2) If the repository requires a username and password, create a credential-storage file to access this repository.

For more information on creating a credential-storage file for Installation Manager, read the IBM Installation Manager Information Center.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutils` command is unable to find the URL that is specified.

- 3) Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being updated.
- 4) Change to the `Installation_Manager_binaries/eclipse/tools` directory, where `Installation_Manager_binaries` is the installation root directory for the Installation Manager.
- 5) Install the fix pack using a response file.

For example:

— **Windows Administrator or non-administrator:**

```
imcl.exe -acceptLicense
input C:\temp\update_response_file.xml
-log C:\temp\update_log.xml
-secureStorageFile C:\IM\credential.store -masterPasswordFile C:\IM\master_password_file.txt
```

— **AIX HP-UX Linux Solaris Administrator:**

```
./imcl -acceptLicense
input /var/temp/update_response_file.xml
-log /var/temp/update_log.xml
-secureStorageFile /var/IM/credential.store -masterPasswordFile /var/IM/master_password_file.txt
```

— **AIX HP-UX Linux Solaris Non-administrator:**

```
./imcl -acceptLicense
input user_home/var/temp/update_response_file.xml
-log user_home/var/temp/update_log.xml
-secureStorageFile user_home/var/IM/credential.store -masterPasswordFile user_home/var/IM/master_password_file.txt
```

## Example

**Windows** The following is an example of a response file for updating the product to a later version.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
<repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85'/>
</server>
<profile id='WebSphere Liberty V8.5'
installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
<install modify='false'>
<offering profile='WebSphere Liberty V8.5' id='com.ibm.websphere.liberty.ND.v85'
version='8.5.5.20101025_2108'/>
</install>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
</agent-input>
```

## Tips:

- The profile ID (`<profile . . . id='profile_ID' . . . .>` and `<offering . . . profile='profile_ID' . . . .>`) can be found when you run the `imcl listInstallationDirectories -verbose` command from the `eclipse/tools` subdirectory in the directory where you installed Installation Manager. It is the same as the package group's name.
- The offering ID (`<offering . . . id='offering_ID' . . . .>`) can be found in WebSphere Application Server product offerings for supported operating systems.
- The *version* is a specific version of the offering to install (8.5.5.20101025\_2108 for example). This specification is optional.

- If *version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
- If *version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
./imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the `installFixes` argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the `installFixes` option defaults to all.
  - If the offering version is specified, the `installFixes` option defaults to none.
-  **8.5.5.2** You can specify additional assets to install from the Liberty Repository. For a list of Liberty Repository assets, see the downloads page on WASdev.net.

To install Liberty Repository assets, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later. Previous versions of Installation Manager do not have the option to install Liberty Repository assets. If you use a response file and did not update Installation Manager to Version 1.6.2 or later, the assets that you specify in the response file are ignored during installation.

If you want to install additional features, specify two extra data key elements in your response file. You can use either the symbolic name or the short name.

The following example installs the Portlet Container and Portlet Serving features using the symbolic name.

```
<data key='user.feature' value='com.ibm.websphere.appserver.portlet-2.0,,com.ibm.websphere.appserver.portletserving-2.0' />
<data key='user.accept.license' value='true' />
```

The following example installs the Portlet Container and Portlet Serving features using the short name:

```
<data key='user.feature' value='portlet-2.0,,portletserving-2.0' />
<data key='user.accept.license' value='true' />
```

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.

**Note:** **8.5.5.3** If you are updating to Version 8.5.5.3 and previously installed Liberty Repository features but do not currently have a connection to the IBM WebSphere Liberty Repository, you cannot update using a response file. Instead, update the product by running the `imcl` command and specifying the `user.feature=""` parameter.

 **8.5.5.4** Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` addon, or install the individual features that you need from the Liberty Repository. See the following topics for more information:

- Installing Liberty Repository assets
- Liberty features

The following example installs the Extended Programming Models using the `user.addon` parameter and the Portlet Container and Portlet Serving features using the `user.feature` parameter with short names:

```
<data key='user.addon' value='extendedPackage-1.0' />
<data key='user.feature' value='portlet-2.0,,portletserving-2.0' />
<data key='user.accept.license' value='true' />
```

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.

 **8.5.5.6** You can also install assets from an instance of the Liberty Asset Repository Service or local directory-based repositories. For more information, see “Installing assets using Installation Manager” on page 1411. Add the repository on `repository` elements. If Installation Manager does not recognize the repository, point directly to the `repository.config` file. When you install assets, the repositories are accessed in the order that you specify them.

```

<server>
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85" />
<repository location="https://your_onprem_asset_repo_url" />
<repository location="D:\IBM\LocalAssetRepo" />

```

**8.5.5.8** <repository location="D:\IBM\LocalAssetRepo2.zip" /> </server> By default, the Liberty Repository is the last of the repositories that are accessed during installation. To disable access to the Liberty Repository, set the **user.useLibertyRepository** parameter to false:

```

<data key='user.addon' value='extendedPackage-1.0' />
<data key='user.feature' value='portlet-2.0,,portlet-serving-2.0' />
<data key='user.useLibertyRepository' value='false' />

```

To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.

- When updating a product, your response file must contain the features that were used in the initial install of the product; otherwise, your update will not occur as intended. If you do not add these features to your response file, Installation Manager assumes you are removing them.

## Uninstalling Liberty fix packs from distributed operating systems using the GUI: **8.5.5.0**

You can roll back WebSphere Application Server Liberty Network Deployment to an earlier version using the Installation Manager GUI.

### Before you begin

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your computer when you install a package. If you change the default setting or delete the saved files, Installation Manager requires access to the repository that was used to install the earlier version.

**Important:** Installation Manager can install any fix-pack level of the product directly without installing the intermediate fix packs; in fact, Installation Manager installs the latest level by default. For example, you can skip fix-pack levels and go from Version 8.5.5.1 directly to Version 8.5.5.5. Keep in mind, however, that later you can not roll back to any level that was skipped. If you directly install to Version 8.5.5.5, for example, you cannot roll back to Version 8.5.5.4. If you skip from Version 8.5.5.1 to Version 8.5.5.5, you can only roll back to Version 8.5.5.1.

**Note:** In WebSphere Application Server Version 8.5.5.0, Liberty was promoted from a feature to an independently installable offering. After updating to WebSphere Application Server Liberty Network Deployment Version 8.5.5.x from Version 8.5.0.x, you can roll back to the Version 8.5.0.x Liberty feature level that you were at before updating. If you previously had a combined full-profile and Liberty-profile installation, the Liberty feature will be reinstalled to the wlp folder when you roll back. Any user data and server configurations will not be restored. If necessary, you can copy them from the backed-up location into the new wlp/usr folder after rollback. If any wlp.bak\_<timestamp> directories are present in your installation image, they will not be affected by the rollback. If you update and roll back multiple times between Version 8.5.0.x and Version 8.5.5.x levels, therefore, you will have multiple wlp.bak\_<timestamp> folders in your installation image. These can always be deleted, copied, or moved without negative impact to your installation.

### Procedure

1. Stop all servers on the WebSphere Application Server Liberty Network Deployment installation that is being modified.
2. Start Installation Manager.
3. Click **Roll Back**.
4. Select the package group to roll back.
5. Click **Next**.

6. Select the version to which you want to roll back under **IBM WebSphere Application Server Liberty Network Deployment**.
7. Click **Next**.
8. Review the summary information, and click **Roll Back**.
  - If the rollback is successful, the program displays a message indicating that the rollback is successful.
  - If the rollback is not successful, click **View Log File** to troubleshoot the problem.
9. Click **Finish**.
10. Click **File > Exit** to close Installation Manager.

### Uninstalling Liberty fix packs from distributed operating systems using the command line:

#### 8.5.5.0

You can roll back WebSphere Application Server Liberty Network Deployment to an earlier version using the Installation Manager command line.

#### Before you begin

**Restriction:** In order to use this procedure, you must have Installation Manager Version 1.6 or later installed on your system.

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your computer when you install a package. If you change the default setting or delete the saved files, Installation Manager requires access to the repository that was used to install the earlier version.

**Note:** In WebSphere Application Server Version 8.5.5.0, Liberty was promoted from a feature to an independently installable offering. After updating to WebSphere Application Server Liberty Network Deployment Version 8.5.5.x from Version 8.5.0.x, you can roll back to the Version 8.5.0.x Liberty feature level that you were at before updating. If you previously had a combined full-profile and Liberty-profile installation, the Liberty feature will be reinstalled to the wlp folder when you roll back. Any user data and server configurations will not be restored. If necessary, you can copy them from the backed-up location into the new wlp/usr folder after rollback. If any wlp.bak\_<timestamp> directories are present in your installation image, they will not be affected by the rollback. If you update and roll back multiple times between Version 8.5.0.x and Version 8.5.5.x levels, therefore, you will have multiple wlp.bak\_<timestamp> folders in your installation image. These can always be deleted, copied, or moved without negative impact to your installation.

#### Procedure

1. Optional: If the repository requires a username and password, create a credential-storage file to access this repository.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the `-keyring` and `-password` options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the `-keyring` and `-password` options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

2. Log on to your system.
3. Stop all servers and applications on the installation that is being rolled back.
4. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
5. Use the `imcl` command to roll back the product.

AIX

HP-UX

Linux

Solaris

```
./imcl rollback offering_ID_offering_version
-repositories source_repository
-installationDirectory installation_directory
-preferences preference_key=value
-properties property_key=value
-secureStorageFile storage_file -masterPasswordFile master_password_file
-acceptLicense
```

Windows

```
imcl.exe rollback offering_ID_offering_version
-repositories source_repository
-installationDirectory installation_directory
-preferences preference_key=value
-properties property_key=value
-secureStorageFile storage_file -masterPasswordFile master_password_file
-acceptLicense
```

#### Tips:

- The *offering\_ID* is the offering ID that is listed in WebSphere Application Server product offerings for supported operating systems.
- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to which to roll back (8.5.5.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the installation rolls back to the previously installed version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the installation rolls back to the specified earlier version of the offering and **no** interim fixes for that version are installed.
- If you previously installed Liberty Repository features and addons but do not have access to a Liberty repository when you rollback your installation, specify the following properties in the response file:
 

```
-properties user.addon="",user.feature=""
```

Specifying these properties enables the product to rollback and uninstalls all features and addons.

- **8.5.5.4** If you are rolling back from Version 8.5.5.4 to Version 8.5.5.3 and you have the Extended Programming Models installed, you might receive errors. To prevent errors, specify a properties parameter, `addon=""`; for example:

AIX

HP-UX

Linux

Solaris

```
./imcl rollback offering_ID_offering_version
-repositories source_repository
-installationDirectory installation_directory
-preferences preference_key=value
-properties user.accept.license=true,user.addon=""
-secureStorageFile storage_file -masterPasswordFile master_password_file
-acceptLicense
```

Windows

```
imcl.exe rollback offering_ID_offering_version
-repositories source_repository
-installationDirectory installation_directory
-preferences preference_key=value
-properties user.accept.license=true,user.addon=""
-secureStorageFile storage_file -masterPasswordFile master_password_file
-acceptLicense
```

For more information on using Installation Manager, read the IBM Installation Manager documentation.

6. Optional: List all installed packages to verify the roll back.

AIX

HP-UX

Linux

Solaris

```
./imcl listInstalledPackages -long
```

Windows

```
imcl.exe listInstalledPackages -long
```

## Uninstalling Liberty fix packs from distributed operating systems by using response files:

8.5.5.0

You can rollback WebSphere Application Server Liberty Network Deployment to an earlier version by using Installation Manager response files.

### Before you begin

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your computer when you install a package. If you change the default setting or delete the saved files, Installation Manager requires access to the repository that was used to install the earlier version.

**Note:** In WebSphere Application Server Version 8.5.5.0, Liberty was promoted from a feature to an independently installable offering. After you update to WebSphere Application Server Liberty Network Deployment Version 8.5.5.x from Version 8.5.0.x, you can rollback to the Version 8.5.0.x Liberty feature level that you were at before you updated. If you previously had a combined full-profile and Liberty-profile installation, the Liberty feature is reinstalled to the wlp folder when you rollback. Any user data and server configurations are not restored. If necessary, you can copy them from the backed-up location into the new wlp/usr folder after rollback. If any wlp.bak\_<timestamp> directories are present in your installation image, they are not affected by the rollback. If you update and rollback multiple times between Version 8.5.0.x and Version 8.5.5.x levels, you have multiple wlp.bak\_<timestamp> folders in your installation image. These folders can always be deleted, copied, or moved without negative impact to your installation.

### Procedure

1. Optional: If the repository requires a username and password, create a credential-storage file to access this repository.

**Tip:** When you create a credential-storage file, append /repository.config at the end of the repository URL location if the **imutilsc** command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see Installation Manager Version 1.6 documentation. For more information on **-keyring** and **-password** options to store credentials in a keyring file, see Installation Manager Version 1.5 documentation.

2. Log on to your system.
3. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being rolled back.
4. Use a response file to roll back the product.

Change to the eclipse/tools subdirectory in the directory where you installed Installation Manager, and roll back the product.

For example:

- **Windows Administrator or non-administrator:**

```
imcl.exe
input C:\temp\rollback_response_file.xml
-log C:\temp\rollback_log.xml
-secureStorageFile C:\IM\credential.store -masterPasswordFile C:\IM\master_password_file.txt
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./imcl
input /var/temp/rollback_response_file.xml
-log /var/temp/rollback_log.xml
-secureStorageFile /var/IM/credential.store -masterPasswordFile /var/IM/master_password_file.txt
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./imcl
input user_home/var/temp/rollback_response_file.xml
-log user_home/var/temp/rollback_log.xml
-secureStorageFile user_home/var/IM/credential.store -masterPasswordFile user_home/var/IM/master_password_file.txt
```

**Note:** The program might write important post-installation instructions to standard output.

For more information on using Installation Manager, read the IBM Installation Manager Information Center.

5. Optional: List all installed packages to verify the rollback.

**AIX HP-UX Linux Solaris**

```
./imcl listInstalledPackages -long
```

**Windows**

```
imcl.exe listInstalledPackages -long
```

**Windows**

### Example

The following is an example of a response file for rolling back the product to an earlier version.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85'/>
</server>
<profile id='WebSphere Liberty V8.5.5' installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
<rollback>
  <offering profile='WebSphere Liberty V8.5.5' id='com.ibm.websphere.liberty.ND.v85' version='8.5.5.20101025_2108' />
</rollback>
</agent-input>
```

### Tips:

- The profile ID (<profile . . . id='profile\_ID' . . . .> and <offering . . . profile='profile\_ID' . . . .>) can be found when you run the imcl listInstallationDirectories -verbose command from the eclipse/tools subdirectory in the directory where you installed Installation Manager. It is the same as the package group's name.
- The offering ID (<offering . . . id='offering\_ID' . . . .>) can be found in WebSphere Application Server product offerings for supported operating systems.
- The *version* is a specific version of the offering to which to roll back (8.5.5.20101025\_2108 for example).

This specification is optional.

- If *version* is **not** specified, the installation rolls back to the previously installed version of the offering and **all** interim fixes for that version are installed.
- If *version* is specified, the installation rolls back to the specified earlier version of the offering and **no** interim fixes for that version are installed.

- If you previously installed Liberty Repository features and add-ons but do not have access to a Liberty repository when you rollback your installation, specify the following properties in the response file:

```
<data key='user.feature' value='' />
<data key='user.addon' value='' />
```

Specifying these properties enables the product to rollback and uninstalls all features and add-ons.

## Upgrading Liberty on distributed operating systems using the GUI

**8.5.5.0**

You can use Installation Manager GUI to upgrade WebSphere Application Server Liberty offerings on distributed operating systems.

### Before you begin

- Make sure that your Installation Manager preferences are pointing to web-based or local repositories that contain the appropriate upgrades for the offering.
- If an interim fix is already installed on the offering that you are trying to upgrade but that specific interim fix is not applicable to the offering to which you want to upgrade, the upgrade will be blocked by Installation Manager. An error message will be generated that indicates that the interim fix is not applicable to the offering. Remove the interim fix before upgrading.

### About this task

You can use Installation Manager to upgrade WebSphere Application Server Liberty offerings in the following paths:

- WebSphere Application Server Liberty Core to WebSphere Application Server Liberty
- WebSphere Application Server Liberty Core to WebSphere Application Server Liberty Network Deployment
- WebSphere Application Server Liberty - Express to WebSphere Application Server Liberty
- WebSphere Application Server Liberty to WebSphere Application Server Liberty Network Deployment
- WebSphere Application Server Liberty Trial to WebSphere Application Server Liberty
- WebSphere Application Server Liberty Core Trial to WebSphere Application Server Liberty Core
- WebSphere Application Server Liberty Network Deployment Trial to WebSphere Application Server Liberty Network Deployment
- WebSphere Application Server Liberty for Developers to WebSphere Application Server Liberty
- WebSphere Application Server Liberty for Developers to WebSphere Application Server Liberty Network Deployment

### Procedure

1. Stop all servers and applications on the WebSphere Application Server Liberty installation that is being upgraded.
2. Start Installation Manager.
3. Click **Install**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

Installation Manager searches its defined repositories for available packages.

4. Select the name of the Liberty offering to which you want to upgrade and the appropriate version, and click **Next**.
5. Accept the terms in the license agreements, and click **Next**.
6. Complete the following actions.

- a. Select **Use the existing package group**.
- b. Select the package group of the product that you want to upgrade.

**Important:** If you select an existing group that cannot be upgraded to the product that you are currently installing, an error will occur.

- c. Click **Next**.
7. Select any features that you want to include in the upgraded installation and click **Next**.
8. Review the summary information, and click **Install**.
  - If the upgrade is successful, the program displays a message indicating that installation is successful.

**Note:** The program might also display important post-installation instructions as well.

  - If the installation is not successful, click **View Log File** to troubleshoot the problem.
9. Click **Finish**.
10. Click **File > Exit** to close Installation Manager.

## Example

Here is an example of how to upgrade a WebSphere Application Server Liberty offering on distributed operating systems using the command line.

- Log on to your system.
- Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
- List the installed packages.

AIX HP-UX Linux Solaris

```
./imcl listInstalledPackages -long
```

Windows

```
imcl.exe listInstalledPackages -long
```

- Use the **imcl install** command to upgrade the installation to a different edition in the same installation location:

AIX HP-UX Linux Solaris

```
./imcl install com.ibm.websphere.liberty.ND.v85
-repositories source_repository -installationDirectory /opt/IBM/WebSphere/Liberty -acceptLicense -showProgress
```

Windows

```
imcl install com.ibm.websphere.liberty.ND.v85
-repositories source_repository -installationDirectory C:\Program Files\IBM\WebSphere\Liberty -acceptLicense -showProgress
```

## Installing and uninstalling SDK Java Technology Edition Version 6.0 for Liberty on distributed operating systems

8.5.5.0

You can install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using Installation Manager.

### About this task

**Note:** **8.5.5.11** Support for using Java SE 6 with WebSphere Liberty ends in September 2017. After the end of support, the Liberty kernel will be recompiled and can no longer run with Java SE 6. If you continue to use Java SE 6 on earlier fix packs after the end of support date, you could expose your environment to security risks.

Java SE 8 is the recommended Java SDK because it provides the latest features and security updates. You can install it by installing the IBM SDK, Java Technology Edition, Version 8 package to the package group that contains WebSphere Liberty.

Perform one of these procedures to install, update, roll back, or uninstall IBM WebSphere SDK Java Technology Edition Version 6.0 using Installation Manager.

**Note:** For information on installing and removing fix packs for WebSphere Application Server LibertyNetwork Deployment on distributed operating systems using the Installation Manager command line, read the following articles in this information center:

- “Installing Liberty fix packs on distributed operating systems using the command line” on page 1200
- “Uninstalling Liberty fix packs from distributed operating systems using the command line” on page 1210

## Procedure

- “Installing IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the GUI” on page 1217
- “Installing IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using response files” on page 1220
- “Installing IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the command line” on page 1219
- “Installing fix packs on IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the GUI” on page 1224
- “Uninstalling fix packs from IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the GUI” on page 1225
- “Uninstalling IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the GUI” on page 1226
- “Uninstalling IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using response files” on page 1227
- “Uninstalling IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the command line” on page 1227

## Results

### Notes on logging and tracing:

- An easy way to view the logs is to open Installation Manager and go to **File > View Log**. An individual log file can be opened by selecting it in the table and then clicking the **Open log file** icon.
- Logs are located in the logs directory of Installation Manager's application data location. For example:

– **Windows** **Administrative installation:**

C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager\logs

– **Windows** **Non-administrative installation:**

C:\Documents and Settings\user\_name\Application Data\IBM\Installation Manager\logs

– **AIX** **HP-UX** **Linux** **Solaris** **Administrative installation:**

/var/ibm/InstallationManager/logs

– **AIX** **HP-UX** **Linux** **Solaris** **Non-administrative installation:**

user\_home/var/ibm/InstallationManager/logs

- The main log files are time-stamped XML files in the logs directory, and they can be viewed using any standard web browser.
- The log.properties file in the logs directory specifies the level of logging or tracing that Installation Manager uses.

## Notes on troubleshooting:

- **HP-UX** By default, some HP-UX systems are configured to not use DNS to resolve host names. This could result in Installation Manager not being able to connect to an external repository. You can ping the repository, but nslookup does not return anything. Work with your system administrator to configure your machine to use DNS, or use the IP address of the repository.
- For more information on using Installation Manager, read the IBM Installation Manager Information Center. Read the release notes to learn more about the latest version of Installation Manager. To access the release notes, complete the following task:
  - **Windows** Click **Start > Programs > IBM Installation Manager > Release Notes**.
  - **AIX** **HP-UX** **Linux** **Solaris** Go to the documentation subdirectory in the directory where Installation Manager is installed, and open the readme.html file.

## Installing IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the GUI:

**8.5.5.0**

You can install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the Installation Manager GUI.

### Before you begin

**Note:** **8.5.5.11** Support for using Java SE 6 with WebSphere Liberty ends in September 2017. After the end of support, the Liberty kernel will be recompiled and can no longer run with Java SE 6. If you continue to use Java SE 6 on earlier fix packs after the end of support date, you could expose your environment to security risks.

Java SE 8 is the recommended Java SDK because it provides the latest features and security updates. You can install it by installing the IBM SDK, Java Technology Edition, Version 8 package to the package group that contains WebSphere Liberty.

1. Prepare your system as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.
2. Install one the following offerings:
  - IBM WebSphere Application Server Liberty
  - IBM WebSphere Application Server Liberty Trial
  - IBM WebSphere Application Server Liberty - Express
  - IBM WebSphere Application Server Liberty Network Deployment
  - IBM WebSphere Application Server Liberty Network Deployment Trial
  - IBM WebSphere Application Server for Developers
  - IBM WebSphere Application Server for Developers (ILAN)

### Procedure

1. Start Installation Manager.

**Tip:** **AIX** **HP-UX** **Linux** **Solaris** You can start Installation Manager in group mode with the `./IBMIM` command.

- Group mode allows users to share packages in a common location and manage them with the same instance of Installation Manager.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

2. Click **Install**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

Installation Manager searches its defined repositories for available packages.

3. Perform the appropriate actions.

a. Select **IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty**.

If you already have IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty installed on a WebSphere Application Server Liberty Network Deployment installation on your system, a message displays indicating that IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty is already installed. To install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty on an installation where it is not yet installed, click **Continue**.

b. Select the fixes to install.

Any recommended fixes are selected by default.

If there are recommended fixes, you can select the option to show only recommended fixes and hide non-recommended fixes.

c. Click **Next**.

**Note:** If you do not have and have not selected an installation of one the following offerings on which to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty, an error dialog displays.

- IBM WebSphere Application Server Liberty
- IBM WebSphere Application Server Liberty Trial
- IBM WebSphere Application Server Liberty - Express
- IBM WebSphere Application Server Liberty Network Deployment
- IBM WebSphere Application Server Liberty Network Deployment Trial
- IBM WebSphere Application Server for Developers
- IBM WebSphere Application Server for Developers (ILAN)

Click **OK**, select an appropriate offering on which to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty, and click **Next**.

4. Select the appropriate WebSphere Application Server Liberty Network Deployment installation on which to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty, and click **Next**.

**Note:** The bit architecture that will be installed, 32 bit or 64 bit, will match the bit selection made during the installation of the Liberty offering. For GUI installations of Liberty offerings, this selection is made on the Location panel. For command-line and response-file installations of Liberty offerings, the default can be overridden using the `cic.selector.arch` property.

5. Click **Next**.

6. Review the summary information, and click **Install**.

- If the installation is successful, the program displays a message indicating that installation is successful.

**Note:** The program might also display important post-installation instructions as well.

- If the installation is not successful, click **View Log File** to troubleshoot the problem.

7. Click **Finish**.

8. Click **File > Exit** to close Installation Manager.

## Installing IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the command line: **8.5.5.0**

You can install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the Installation Manager command line.

### Before you begin

**Note:** **8.5.5.11** Support for using Java SE 6 with WebSphere Liberty ends in September 2017. After the end of support, the Liberty kernel will be recompiled and can no longer run with Java SE 6. If you continue to use Java SE 6 on earlier fix packs after the end of support date, you could expose your environment to security risks.

Java SE 8 is the recommended Java SDK because it provides the latest features and security updates. You can install it by installing the IBM SDK, Java Technology Edition, Version 8 package to the package group that contains WebSphere Liberty.

1. Prepare your system as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.
2. Install one the following offerings:
  - IBM WebSphere Application Server Liberty
  - IBM WebSphere Application Server Liberty Trial
  - IBM WebSphere Application Server Liberty - Express
  - IBM WebSphere Application Server Liberty Network Deployment
  - IBM WebSphere Application Server Liberty Network Deployment Trial
  - IBM WebSphere Application Server for Developers
  - IBM WebSphere Application Server for Developers (ILAN)

### Procedure

1. Optional: If the repository requires a username and password, create a credential-storage file to access this repository.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the `-keyring` and `-password` options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the `-keyring` and `-password` options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

2. Log on to your system.
3. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
4. Verify that the repository is available.

Windows

```
imcl.exe listAvailablePackages -repositories path_to_repository
```

AIX

HP-UX

Linux

Solaris

```
./imcl listAvailablePackages -repositories path_to_repository
```

You should see one or more levels of the offering.

## 5. Use the **imcl** command to install the offering.

Windows

```
imcl.exe install com.ibm.websphere.liberty.IBMJAVA.v60_offering_version
-repositories source_repository
-installationDirectory installation_directory
-secureStorageFile storage_file -masterPasswordFile master_password_file
```

AIX

HP-UX

Linux

Solaris

```
./imcl install com.ibm.websphere.liberty.IBMJAVA.v60_offering_version
-repositories source_repository
-installationDirectory installation_directory
-secureStorageFile storage_file -masterPasswordFile master_password_file
```

**Note:** The bit architecture that will be installed, 32 bit or 64 bit, will match the bit selection made during the installation of the Liberty offering. For GUI installations of Liberty offerings, this selection is made on the Location panel. For command-line and response-file installations of Liberty offerings, the default can be overridden using the `cic.selector.arch` property.

### Tips:

- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.5.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the `-installFixes` option defaults to all.
  - If the offering version is specified, the `-installFixes` option defaults to none.
- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lfiles` or `product_name/lfiles` subdirectory of the installation image or repository for this offering.
- The program might write important post-installation instructions to standard output.

For more information on using the **imcl** command, see the IBM Installation Manager Information Center.

## Installing IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using response files:

8.5.5.0

You can install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using Installation Manager response files.

### Before you begin

**Note:** 8.5.5.11 Support for using Java SE 6 with WebSphere Liberty ends in September 2017. After the end of support, the Liberty kernel will be recompiled and can no longer run with Java SE 6. If you continue to use Java SE 6 on earlier fix packs after the end of support date, you could expose your environment to security risks.

Java SE 8 is the recommended Java SDK because it provides the latest features and security updates. You can install it by installing the IBM SDK, Java Technology Edition, Version 8 package to the package group that contains WebSphere Liberty.

1. Prepare your system as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.
2. Install one the following offerings:
  - IBM WebSphere Application Server Liberty
  - IBM WebSphere Application Server Liberty Trial
  - IBM WebSphere Application Server Liberty - Express
  - IBM WebSphere Application Server Liberty Network Deployment
  - IBM WebSphere Application Server Liberty Network Deployment Trial
  - IBM WebSphere Application Server for Developers
  - IBM WebSphere Application Server for Developers (ILAN)

### About this task

Using Installation Manager, you can work with response files to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

### Procedure

1. Optional: **Record a response file to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty:** On one of your systems, perform the following actions to record a response file that will install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty.
  - a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.
  - b. Start Installation Manager from the command line using the `-record` option.

For example:

- **Windows Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"  
-record C:\temp\install_response_file.xml
```
- **AIX HP-UX Linux Solaris Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry  
-record /var/temp/install_response_file.xml
```
- **AIX HP-UX Linux Solaris Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry  
-record user_home/var/temp/install_response_file.xml
```

**Tip:** When you record a new response file, you can specify the `-skipInstall` parameter. Using this parameter has the following benefits:

- No files are actually installed, and this speeds up the recording.
- If you use a temporary data location with the `-skipInstall` parameter, Installation Manager writes the installation registry to the specified data location while recording. When you start Installation Manager again without the `-skipInstall` parameter, you then can use your response file to install against the real installation registry.

The `-skipInstall` operation should not be used on the actual agent data location used by Installation Manager. This is unsupported. Use a clean writable location, and reuse that location for future recording sessions.

For more information, read the IBM Installation Manager Information Center.

- c. Add the appropriate repositories to your Installation Manager preferences.

- 1) Click **File > Preferences**.
- 2) Select **Repositories**.
- 3) Perform the following actions for each repository:
  - a) Click **Add Repository**.
  - b) Enter the path to the repository.config file in the remote web-based repository or the local directory into which you unpacked the repository files.

For example:

- Remote repositories:

`https://downloads.mycorp.com:8080/WAS_85_repository`

or

`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v60`

- Local repositories:

– **Windows** C:\repositories\jdk6\local-repositories

– **AIX** **HP-UX** **Linux** **Solaris** /var/repositories/jdk6/local-repositories

- c) Click **OK**.
- 4) Click **Apply**.
- 5) Click **OK**.
- d. Click **Install**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

Installation Manager searches its defined repositories for available packages.

- e. Perform the appropriate actions.

- 1) Select **IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty**.

If you already have IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty installed on your system in the targeted location, a message displays indicating that IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty is already installed. To install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty where it is not yet installed, click **Continue**.

- 2) Select the fixes to install.

Any recommended fixes are selected by default.

If there are recommended fixes, you can select the option to show only recommended fixes and hide non-recommended fixes.

- 3) Click **Next**.

**Note:** If you do not have and have not selected an installation of one the following offerings on which to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty, an error dialog displays.

- IBM WebSphere Application Server Liberty
- IBM WebSphere Application Server Liberty Trial
- IBM WebSphere Application Server Liberty - Express
- IBM WebSphere Application Server Liberty Network Deployment
- IBM WebSphere Application Server Liberty Network Deployment Trial
- IBM WebSphere Application Server for Developers
- IBM WebSphere Application Server for Developers (ILAN)

Click **OK**, select an appropriate offering on which to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty, and click **Next**.

- f. Select the appropriate WebSphere Application Server Liberty Network Deployment installation on which to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty, and click **Next**.

**Note:** The bit architecture that will be installed, 32 bit or 64 bit, will match the bit selection made during the installation of the Liberty offering. For GUI installations of Liberty offerings, this selection is made on the Location panel. For command-line and response-file installations of Liberty offerings, the default can be overridden using the `cic.selector.arch` property.

- g. Click **Next**.
- h. Review the summary information, and click **Install**.
  - If the installation is successful, the program displays a message indicating that installation is successful.

**Note:** The program might also display important post-installation instructions as well.

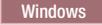
- If the installation is not successful, click **View Log File** to troubleshoot the problem.
- i. Click **Finish**.
  - j. Click **File > Exit** to close Installation Manager.
  - k. Optional: If you are using an authenticated remote repository, create a credential-storage file for silent installation.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

## 2. Use the response files to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty:

- a. Optional: **Use the response file to install the credential-storage file:** Go to a command line on each of the systems on which you want to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the credential-storage file.

For example:

-  **Administrator or non-administrator:**

```
imcl.exe
input C:\temp\credentialstorage_response_file.xml
-log C:\temp\credentialstorage_log.xml
```

-     **Administrator:**

```
./imcl
input /var/temp/credentialstorage_response_file.xml
-log /var/temp/credentialstorage_log.xml
```

-     **Non-administrator:**

```
./imcl
input user_home/var/temp/credentialstorage_response_file.xml
-log user_home/var/temp/credentialstorage_log.xml
```

- b. **Use the response file to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty:** Go to a command line on each of the systems on which you want to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty.

For example:

- **Windows Administrator or non-administrator:**

```
imcl.exe
input C:\temp\install_response_file.xml
-log C:\temp\install_log.xml
-secureStorageFile C:\IM\credential.store -masterPasswordFile C:\IM\master_password_file.txt
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./imcl
input /var/temp/install_response_file.xml
-log /var/temp/install_log.xml
-secureStorageFile /var/IM/credential.store -masterPasswordFile /var/IM/master_password_file.txt
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./imcl
input user_home/var/temp/install_response_file.xml
-log user_home/var/temp/install_log.xml
-secureStorageFile user_home/var/IM/credential.store -masterPasswordFile user_home/var/IM/master_password_file.txt
```

### Notes:

- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lafiles` or `product_name/lafiles` subdirectory of the installation image or repository for this offering.
- The program might write important post-installation instructions to standard output.

Read the IBM Installation Manager Information Center for more information.

### Example

**Windows** The following is an example of a response file for installing IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean="true" temporary="true">
<server>
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v60" />
</server>
<install modify='false'>
<offering id='com.ibm.websphere.liberty.IBMJAVA.v60'
profile='WebSphere Liberty V8.5' installFixes='none' />
</install>
<profile id='WebSphere Liberty V8.5' installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
</agent-input>
```

### Installing fix packs on IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the GUI: **8.5.5.0**

You can update IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty to a later version using the Installation Manager GUI.

### Before you begin

**Note:** **8.5.5.11** Support for using Java SE 6 with WebSphere Liberty ends in September 2017. After the end of support, the Liberty kernel will be recompiled and can no longer run with Java SE 6. If you continue to use Java SE 6 on earlier fix packs after the end of support date, you could expose your environment to security risks.

Java SE 8 is the recommended Java SDK because it provides the latest features and security updates. You can install it by installing the IBM SDK, Java Technology Edition, Version 8 package to the package group that contains WebSphere Liberty.

Make sure that the web-based or local service repository location is listed and checked or that the **Search service repositories during installation and updates** option is selected on the Repositories panel in your Installation Manager preferences. For more information on using service repositories with Installation Manager, read the IBM Installation Manager Information Center.

## About this task

**Note:** For information on installing and removing fix packs for WebSphere Application Server LibertyNetwork Deployment on distributed operating systems using the Installation Manager command line, read the following articles in this information center:

- “Installing Liberty fix packs on distributed operating systems using the command line” on page 1200
- “Uninstalling Liberty fix packs from distributed operating systems using the command line” on page 1210

## Procedure

1. Start Installation Manager.
2. Click **Update**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you use to access protected IBM software websites.

3. Select the package group to update.

**Tip:** If you select **Update all**, Installation Manager will search all of the added and predefined repositories for recommended updates to all of the package groups that it has installed.

- Use this feature only if you have full control over which fixes are contained in the targeted repositories.
  - If you create and point to a set of custom repositories that include only the specific recommended fixes that you want to install, you should be able to use this feature confidently.
  - If you enable searching service repositories or install fixes directly from other live web-based repositories, you might not want to select this option so that you can select only the fixes that you want to install for each offering on subsequent panels.
- If you select **Update all**, Installation Manager will install only the recommended updates to all of the package groups; it will not allow you to select non-recommended fixes for installation. If you want to install non-recommended fixes, perform the following actions:
  - a. On this panel, clear the **Update all** check box and select an offering to update.
  - b. On the next panel, clear the option to show only recommended fixes and then select the fixes that you want to install.

4. Click **Next**.
5. Select the version to which you want to update under **IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty**.
6. Click **Next**.
7. Accept the terms in the license agreements, and click **Next**.
8. Review the summary information, and click **Update**.
  - If the installation is successful, the program displays a message indicating that installation is successful.
  - If the installation is not successful, click **View Log File** to troubleshoot the problem.
9. Click **Finish**.
10. Click **File > Exit** to close Installation Manager.

**Uninstalling fix packs from IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the GUI:** **8.5.5.0**

You can roll back IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty to an earlier version using the Installation Manager GUI.

## Before you begin

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your computer when you install a package. If you change the default setting or delete the saved files, Installation Manager requires access to the repository that was used to install the earlier version.

## About this task

**Note:** For information on installing and removing fix packs for WebSphere Application Server Liberty Network Deployment on distributed operating systems using the Installation Manager command line, read the following articles in this information center:

- “Installing Liberty fix packs on distributed operating systems using the command line” on page 1200
- “Uninstalling Liberty fix packs from distributed operating systems using the command line” on page 1210

## Procedure

1. Stop all servers on the installation that is being modified.
2. Start Installation Manager.
3. Click **Roll Back**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you use to access protected IBM software websites.

4. Select the package group to roll back.
5. Click **Next**.
6. Select the version to which you want to roll back under **IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty**.
7. Click **Next**.
8. Review the summary information, and click **Roll Back**.
  - If the rollback is successful, the program displays a message indicating that the rollback is successful.
  - If the rollback is not successful, click **View Log File** to troubleshoot the problem.
9. Click **Finish**.
10. Click **File > Exit** to close Installation Manager.

## Uninstalling IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the GUI:

**8.5.5.0**

Use the Installation Manager GUI to uninstall IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty.

## Before you begin

Make sure that no commands or server profiles are using IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty before uninstalling it. Server profiles using IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty will not function if it is uninstalled.

## Procedure

1. Log on to your system.
2. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.

3. Start Installation Manager.
4. Click **Uninstall**.
5. In the **Uninstall Packages** window, perform the following actions.
  - a. Select **IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty**.
  - b. Click **Next**.
6. Review the summary information.
7. Click **Uninstall**.
  - If the uninstallation is successful, the program displays a message that indicates success.
  - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
8. Click **Finish**.
9. Click **File > Exit** to close Installation Manager.

**Uninstalling IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the command line:** **8.5.5.0**

You can uninstall IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using the Installation Manager command line.

### Before you begin

Make sure that no commands or server profiles are using IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty before uninstalling it. Server profiles using IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty will not function if it is uninstalled.

### Procedure

1. Log on to your system.
2. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
3. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
4. Use the `imcl` command to uninstall the offering.

Windows

```
imcl.exe uninstall com.ibm.websphere.liberty.IBMJAVA.v60
-installationDirectory installation_directory
```

AIX

HP-UX

Linux

Solaris

```
./imcl uninstall com.ibm.websphere.liberty.IBMJAVA.v60
-installationDirectory installation_directory
```

Go to the IBM Installation Manager Information Center for more information.

**Uninstalling IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using response files:** **8.5.5.0**

You can uninstall IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty using Installation Manager response files.

### Before you begin

Make sure that no commands or server profiles are using IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty before uninstalling it. Server profiles using IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty will not function if it is uninstalled.

**Optional:** Perform or record the installation of Installation Manager and installation of IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty to a temporary installation registry on one of your systems so that you can use this temporary registry to record the uninstallation without using the standard registry where Installation Manager is installed.

## About this task

Using Installation Manager, you can work with response files to uninstall IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

## Procedure

1. **Optional: Record a response file to uninstall IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty:** On one of your systems, perform the following actions to record a response file that will uninstall IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty:
  - a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.
  - b. Start Installation Manager from the command line using the `-record` option.

For example:

- **Windows Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"  
-record C:\temp\uninstall_response_file.xml
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry  
-record /var/temp/uninstall_response_file.xml
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry  
-record user_home/var/temp/uninstall_response_file.xml
```

**Tip:** If you choose to use the `-skipInstall` parameter with a temporary installation registry created as described in *Before you begin*, Installation Manager uses the temporary installation registry while recording the response file. It is important to note that when the `-skipInstall` parameter is specified, no packages are installed or uninstalled. All of the actions that you perform in Installation Manager simply update the installation data that is stored in the specified temporary registry. After the response file is generated, it can be used to uninstall IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty, removing the files and updating the standard installation registry.

The `-skipInstall` operation should not be used on the actual agent data location used by Installation Manager. This is unsupported. Use a clean writable location, and reuse that location for future recording sessions.

For more information, read the IBM Installation Manager Information Center.

- c. Click **Uninstall**.
- d. In the **Uninstall Packages** window, perform the following actions.
  - 1) Select **IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty**.
  - 2) Click **Next**.
- e. Review the summary information.
- f. Click **Uninstall**.
  - If the uninstallation is successful, the program displays a message that indicates success.
  - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
- g. Click **Finish**.

h. Click **File > Exit** to close Installation Manager.

2. **Use the response file to uninstall IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty:** From a command line on each of the systems from which you want to uninstall IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager and use the response file that you created to uninstall IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty.

For example:

- **Windows Administrator or non-administrator:**

```
imcl.exe
input C:\temp\uninstall_response_file.xml
-log C:\temp\uninstall_log.xml
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./imcl
input /var/temp/uninstall_response_file.xml
-log /var/temp/uninstall_log.xml
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./imcl
input user_home/var/temp/uninstall_response_file.xml
-log user_home/var/temp/uninstall_log.xml
```

Go to the IBM Installation Manager Information Center for more information.

3. **Optional: List all installed packages to verify the uninstallation.**

**AIX HP-UX Linux Solaris**

```
./imcl listInstalledPackages
```

**Windows**

```
imcl listInstalledPackages
```

**Windows**

## Example

The following is an example of a response file for uninstalling IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean='true' temporary='true'>
<uninstall modify='false'>
<offering id='com.ibm.websphere.liberty.IBMJAVA.v60'
  profile='WebSphere Liberty V8.5' />
</uninstall>
<profile id='WebSphere Liberty V8.5'
  installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
</agent-input>
```

## Installing and uninstalling SDK Java Technology Edition Version 7.0 or 7.1 for Liberty on distributed operating systems

**8.5.5.0**

You can install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using Installation Manager.

### About this task

Perform one of these procedures to install, update, roll back, or uninstall IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using Installation Manager.

**8.5.5.2**

You can download and install IBM WebSphere SDK Java Technology Edition Version 7.1. This version is only available from the web. This version is not available on the physical media. You have the following installation options:

- Download the installation files from the IBM Fix Central website and use a local installation.
- Access the live repositories and use your IBM Software ID for a web-based installation.

## Procedure

- “Installing IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the GUI” on page 1231
- “Installing IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using response files” on page 1234
- “Installing IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the command line” on page 1232
- “Installing fix packs on IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the GUI” on page 1239
- “Uninstalling fix packs from IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the GUI” on page 1240
- “Uninstalling IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the GUI” on page 1241
- “Uninstalling IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using response files” on page 1242
- “Uninstalling IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the command line” on page 1241

## Results

### Notes on logging and tracing:

- An easy way to view the logs is to open Installation Manager and go to **File > View Log**. An individual log file can be opened by selecting it in the table and then clicking the **Open log file** icon.
- Logs are located in the logs directory of Installation Manager's application data location. For example:

– **Windows** **Administrative installation:**

C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager\logs

– **Windows** **Non-administrative installation:**

C:\Documents and Settings\user\_name\Application Data\IBM\Installation Manager\logs

– **AIX** **HP-UX** **Linux** **Solaris** **Administrative installation:**

/var/ibm/InstallationManager/logs

– **AIX** **HP-UX** **Linux** **Solaris** **Non-administrative installation:**

user\_home/var/ibm/InstallationManager/logs

- The main log files are time-stamped XML files in the logs directory, and they can be viewed using any standard web browser.
- The log.properties file in the logs directory specifies the level of logging or tracing that Installation Manager uses.

### Notes on troubleshooting:

- **HP-UX** By default, some HP-UX systems are configured to not use DNS to resolve host names. This could result in Installation Manager not being able to connect to an external repository. You can ping the repository, but nslookup does not return anything. Work with your system administrator to configure your machine to use DNS, or use the IP address of the repository.
- For more information on using Installation Manager, read the IBM Installation Manager Information Center.

Read the release notes to learn more about the latest version of Installation Manager. To access the release notes, complete the following task:

- **Windows** Click **Start > Programs > IBM Installation Manager > Release Notes**.
- **AIX** **HP-UX** **Linux** **Solaris** Go to the documentation subdirectory in the directory where Installation Manager is installed, and open the `readme.html` file.

## Installing IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the GUI:

### 8.5.5.0

You can install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the Installation Manager GUI.

### Before you begin

1. Prepare your system as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.
2. Install one the following offerings:
  - IBM WebSphere Application Server Liberty
  - IBM WebSphere Application Server Liberty Trial
  - IBM WebSphere Application Server Liberty Core
  - IBM WebSphere Application Server Liberty Core Trial
  - IBM WebSphere Application Server Liberty - Express
  - IBM WebSphere Application Server Liberty Network Deployment
  - IBM WebSphere Application Server Liberty Network Deployment Trial
  - IBM WebSphere Application Server Liberty for Developers
  - IBM WebSphere Application Server Liberty for Developers (ILAN)

### 8.5.5.2

You can download and install IBM WebSphere SDK Java Technology Edition Version 7.1. This version is only available from the web. You have the following installation options:

- Download the installation files from the IBM Fix Central website and use a local installation.
- Access the live repositories and use your IBM Software ID for a web-based installation.

### Procedure

1. Start Installation Manager.

**Tip:** **AIX** **HP-UX** **Linux** **Solaris** You can start Installation Manager in group mode with the `./IBMIM` command.

- Group mode allows users to share packages in a common location and manage them with the same instance of Installation Manager.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

2. Click **Install**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

Installation Manager searches its defined repositories for available packages.

3. Perform the appropriate actions.
  - a. Select **IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty** and the appropriate version.

If you already have IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty installed on a WebSphere Application Server Liberty Network Deployment installation on your system, a message displays indicating that IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty is already installed. To install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty on an installation where it is not yet installed, click **Continue**.

- b. Select the fixes to install.

Any recommended fixes are selected by default.

If there are recommended fixes, you can select the option to show only recommended fixes and hide non-recommended fixes.

- c. Click **Next**.

**Note:** If you do not have and have not selected a Version 8.5 installation of one the following offerings on which to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty, an error dialog displays.

- IBM WebSphere Application Server Liberty
- IBM WebSphere Application Server Liberty Trial
- IBM WebSphere Application Server Liberty Core
- IBM WebSphere Application Server Liberty Core Trial
- IBM WebSphere Application Server Liberty - Express
- IBM WebSphere Application Server Liberty Network Deployment
- IBM WebSphere Application Server Liberty Network Deployment Trial
- IBM WebSphere Application Server Liberty for Developers
- IBM WebSphere Application Server Liberty for Developers (ILAN)

Click **OK**, select an appropriate offering on which to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty, and click **Next**.

4. Select the appropriate installation on which to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty, and click **Next**.

**Note:** The bit architecture that will be installed, 32 bit or 64 bit, will match the bit selection made during the installation of the Liberty offering. For GUI installations of Liberty offerings, this selection is made on the Location panel. For command-line and response-file installations of Liberty offerings, the default can be overridden using the `cic.selector.arch` property.

5. Click **Next**.

6. Review the summary information, and click **Install**.

- If the installation is successful, the program displays a message indicating that installation is successful.

**Note:** The program might also display important post-installation instructions as well.

- If the installation is not successful, click **View Log File** to troubleshoot the problem.

7. Click **Finish**.

8. Click **File > Exit** to close Installation Manager.

**Installing IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the command line:** `8.5.5.0`

You can install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the Installation Manager command line.

## Before you begin

1. Prepare your system as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.
2. Install one the following offerings:
  - IBM WebSphere Application Server Liberty
  - IBM WebSphere Application Server Liberty Trial
  - IBM WebSphere Application Server Liberty Core
  - IBM WebSphere Application Server Liberty Core Trial
  - IBM WebSphere Application Server Liberty - Express
  - IBM WebSphere Application Server Liberty Network Deployment
  - IBM WebSphere Application Server Liberty Network Deployment Trial
  - IBM WebSphere Application Server Liberty for Developers
  - IBM WebSphere Application Server Liberty for Developers (ILAN)

### 8.5.5.2

You can download and install IBM WebSphere SDK Java Technology Edition Version 7.1. This version is only available from the web. You have the following installation options:

- Download the installation files from the IBM Fix Central website and use a local installation.
- Access the live repositories and use your IBM Software ID for a web-based installation.

## Procedure

1. Optional: If the repository requires a username and password, create a credential-storage file to access this repository.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the `-keyring` and `-password` options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the `-keyring` and `-password` options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

2. Log on to your system.
3. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
4. Verify that the repository is available.

Windows

```
imcl.exe listAvailablePackages -repositories path_to_repository
```

AIX

HP-UX

Linux

Solaris

```
./imcl listAvailablePackages -repositories path_to_repository
```

You should see one or more levels of the offering.

5. Use the `imcl` command to install the offering.

Windows

8.5.5.0

```
imcl.exe install com.ibm.websphere.liberty.IBMJAVA.v70_offering_version  
-repositories source_repository  
-installationDirectory installation_directory  
-secureStorageFile storage_file -masterPasswordFile master_password_file
```

## 8.5.5.2

```
imcl.exe install com.ibm.websphere.liberty.IBMJAVA.v71_offering_version
-repositories source_repository
-installationDirectory installation_directory
-secureStorageFile storage_file -masterPasswordFile master_password_file
```

AIX

HP-UX

Linux

Solaris

8.5.5.0

```
./imcl install com.ibm.websphere.liberty.IBMJAVA.v70_offering_version
-repositories source_repository
-installationDirectory installation_directory
-secureStorageFile storage_file -masterPasswordFile master_password_file
```

## 8.5.5.2

```
./imcl install com.ibm.websphere.liberty.IBMJAVA.v71_offering_version
-repositories source_repository
-installationDirectory installation_directory
-secureStorageFile storage_file -masterPasswordFile master_password_file
```

The value of the **-installationDirectory** parameter should be the location of an existing Liberty installation. The SDK offering will be installed into the `<liberty_home>\java\java_1.7_32` or `<liberty_home>\java\java_1.7_64` folder, depending on whether the installation location was configured to be 32-bit or 64-bit when the Liberty offering was initially installed.

**Note:** The bit architecture that will be installed, 32 bit or 64 bit, will match the bit selection made during the installation of the Liberty offering. For GUI installations of Liberty offerings, this selection is made on the Location panel. For command-line and response-file installations of Liberty offerings, the default can be overridden using the `cic.selector.arch` property.

### Tips:

- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.0.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the `-installFixes` option defaults to all.
  - If the offering version is specified, the `-installFixes` option defaults to none.
- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lfiles` or `product_name/lfiles` subdirectory of the installation image or repository for this product.
- The program might write important post-installation instructions to standard output.

For more information on using the **imcl** command, see the IBM Installation Manager Information Center.

## Installing IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using response files: 8.5.5.0

You can install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using Installation Manager response files.

## Before you begin

1. Prepare your system as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.
2. Install one the following offerings:
  - IBM WebSphere Application Server Liberty
  - IBM WebSphere Application Server Liberty Trial
  - IBM WebSphere Application Server Liberty Core
  - IBM WebSphere Application Server Liberty Core Trial
  - IBM WebSphere Application Server Liberty - Express
  - IBM WebSphere Application Server Liberty Network Deployment
  - IBM WebSphere Application Server Liberty Network Deployment Trial
  - IBM WebSphere Application Server Liberty for Developers
  - IBM WebSphere Application Server Liberty for Developers (ILAN)

## About this task

Using Installation Manager, you can work with response files to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

### 8.5.5.2

You can download and install IBM WebSphere SDK Java Technology Edition Version 7.1. This version and later versions are only available from the web. You have the following installation options:

- Download the installation files from the IBM Fix Central website and use a local installation.
- Access the live repositories and use your IBM Software ID for a web-based installation.

## Procedure

1. Optional: **Record a response file to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty:** On one of your systems, perform the following actions to record a response file that will install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty.
  - a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.
  - b. Start Installation Manager from the command line using the `-record` option.

For example:

- **Windows Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"  
-record C:\temp\install_response_file.xml
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry  
-record /var/temp/install_response_file.xml
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry  
-record user_home/var/temp/install_response_file.xml
```

**Tip:** When you record a new response file, you can specify the `-skipInstall` parameter. Using this parameter has the following benefits:

- No files are actually installed, and this speeds up the recording.
- If you use a temporary data location with the `-skipInstall` parameter, Installation Manager writes the installation registry to the specified data location while recording. When you start

Installation Manager again without the `-skipInstall` parameter, you then can use your response file to install against the real installation registry.

The `-skipInstall` operation should not be used on the actual agent data location used by Installation Manager. This is unsupported. Use a clean writable location, and re-use that location for future recording sessions.

For more information, read the IBM Installation Manager Information Center.

- c. Add the appropriate repositories to your Installation Manager preferences.
  - 1) Click **File > Preferences**.
  - 2) Select **Repositories**.
  - 3) Perform the following actions for each repository:
    - a) Click **Add Repository**.
    - b) Enter the path to the `repository.config` file in the remote web-based repository or the local directory into which you unpacked the repository files.

For example:

- Remote repositories:

[https://downloads.mycorp.com:8080/WAS\\_85\\_repository](https://downloads.mycorp.com:8080/WAS_85_repository)

or **8.5.5.1**

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v70>

**8.5.5.2**

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v71>

- Local repositories:

– **Windows** C:\repositories\jdk7\local-repositories

– **AIX** **HP-UX** **Linux** **Solaris** /var/repositories/jdk7/local-repositories

- c) Click **OK**.
- 4) Click **Apply**.
- 5) Click **OK**.
- d. Click **Install**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

Installation Manager searches its defined repositories for available packages.

- e. Perform the appropriate actions.
  - 1) Select **IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty**.

If you already have IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty installed on a WebSphere Application Server LibertyNetwork Deployment installation on your system in the targeted location, a message displays indicating that IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty is already installed. To install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 on a WebSphere Application Server Liberty Network Deployment installation where it is not yet installed, click **Continue**.
  - 2) Select the fixes to install.

Any recommended fixes are selected by default.

If there are recommended fixes, you can select the option to show only recommended fixes and hide non-recommended fixes.
  - 3) Click **Next**.

**Note:** If you do not have and have not selected an installation of one the following offerings on which to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty, an error dialog displays.

- IBM WebSphere Application Server Liberty
- IBM WebSphere Application Server Liberty Trial
- IBM WebSphere Application Server Liberty Core
- IBM WebSphere Application Server Liberty Core Trial
- IBM WebSphere Application Server Liberty - Express
- IBM WebSphere Application Server Liberty Network Deployment
- IBM WebSphere Application Server Liberty Network Deployment Trial
- IBM WebSphere Application Server Liberty for Developers
- IBM WebSphere Application Server Liberty for Developers (ILAN)

Click **OK**, select an appropriate offering on which to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty, and click **Next**.

- f. Select the appropriate WebSphere Application Server Liberty Network Deployment installation on which to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty, and click **Next**.

**Note:** The bit architecture that will be installed, 32 bit or 64 bit, will match the bit selection made during the installation of the Liberty offering. For GUI installations of Liberty offerings, this selection is made on the Location panel. For command-line and response-file installations of Liberty offerings, the default can be overridden using the `cic.selector.arch` property.

- g. Click **Next**.
- h. Review the summary information, and click **Install**.
  - If the installation is successful, the program displays a message indicating that installation is successful.

**Note:** The program might also display important post-installation instructions as well.

- If the installation is not successful, click **View Log File** to troubleshoot the problem.
- i. Click **Finish**.
- j. Click **File > Exit** to close Installation Manager.
- k. Optional: If you are using an authenticated remote repository, create a credential-storage file for silent installation.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

## 2. Use the response files to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty:

- a. Optional: **Use the response file to install the credential-storage file:** Go to a command line on each of the systems on which you want to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the credential-storage file.

For example:

- **Windows Administrator or non-administrator:**

```
imcl.exe
input C:\temp\credentialstorage_response_file.xml
-log C:\temp\credentialstorage_log.xml
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./imcl
input /var/temp/credentialstorage_response_file.xml
-log /var/temp/credentialstorage_log.xml
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./imcl
input user_home/var/temp/credentialstorage_response_file.xml
-log user_home/var/temp/credentialstorage_log.xml
```

- Use the response file to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty:** Go to a command line on each of the systems on which you want to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty, change to the eclipse/tools subdirectory in the directory where you installed Installation Manager, and install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty.

For example:

- **Windows Administrator or non-administrator:**

```
imcl.exe
input C:\temp\install_response_file.xml
-log C:\temp\install_log.xml
-secureStorageFile C:\IM\credential.store -masterPasswordFile C:\IM\master_password_file.txt
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./imcl
input /var/temp/install_response_file.xml
-log /var/temp/install_log.xml
-secureStorageFile /var/IM/credential.store -masterPasswordFile /var/IM/master_password_file.txt
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./imcl
input user_home/var/temp/install_response_file.xml
-log user_home/var/temp/install_log.xml
-secureStorageFile user_home/var/IM/credential.store -masterPasswordFile user_home/var/IM/master_password_file.txt
```

#### Notes:

- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the lafiles or *product\_name/lafiles* subdirectory of the installation image or repository for this product.
- The program might write important post-installation instructions to standard output.

Read the IBM Installation Manager Information Center.

#### Example

Windows

**8.5.5.1**

The following is an example of a response file for installing IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean="true" temporary="true">
<server>
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v70" />
</server>
<install modify='false'>
<offering id='com.ibm.websphere.liberty.IBMJAVA.v70'
profile='WebSphere Liberty V8.5' installFixes='none'/>
</install>
<profile id='WebSphere Liberty V8.5' installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
</agent-input>
```

Windows

**8.5.5.2**

The following is an example of a response file for installing IBM WebSphere SDK Java Technology Edition Version 7.1 for Liberty.

```

<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean="true" temporary="true">
<server>
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v71" />
</server>
<install modify='false'>
<offering id='com.ibm.websphere.liberty.IBMJAVA.v71'
profile='WebSphere Liberty V8.5' installFixes='none' />
</install>
<profile id='WebSphere Liberty V8.5' installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
</agent-input>

```

## Installing fix packs on IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the GUI: **8.5.5.0**

You can update IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty to a later version using the Installation Manager GUI.

### Before you begin

Make sure that the web-based or local service repository location is listed and checked or that the **Search service repositories during installation and updates** option is selected on the Repositories panel in your Installation Manager preferences. For more information on using service repositories with Installation Manager, read the IBM Installation Manager Information Center.

### About this task

**Note:** For information on installing and removing fix packs for WebSphere Application Server Liberty Network Deployment on distributed operating systems using the Installation Manager command line, read the following articles in this information center:

- “Installing Liberty fix packs on distributed operating systems using the command line” on page 1200
- “Uninstalling Liberty fix packs from distributed operating systems using the command line” on page 1210

### Procedure

1. Start Installation Manager.
2. Click **Update**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you use to access protected IBM software websites.

3. Select the package group to update.

**Tip:** If you select **Update all**, Installation Manager will search all of the added and predefined repositories for recommended updates to all of the package groups that it has installed.

- Use this feature only if you have full control over which fixes are contained in the targeted repositories.
  - If you create and point to a set of custom repositories that include only the specific recommended fixes that you want to install, you should be able to use this feature confidently.
  - If you enable searching service repositories or install fixes directly from other live web-based repositories, you might not want to select this option so that you can select only the fixes that you want to install for each offering on subsequent panels.
- If you select **Update all**, Installation Manager will install only the recommended updates to all of the package groups; it will not allow you to select non-recommended fixes for installation. If you want to install non-recommended fixes, perform the following actions:
  - a. On this panel, clear the **Update all** check box and select an offering to update.

- b. On the next panel, clear the option to show only recommended fixes and then select the fixes that you want to install.
4. Click **Next**.
5. Select the version to which you want to update under **IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty**.
6. Click **Next**.
7. Accept the terms in the license agreements, and click **Next**.
8. Review the summary information, and click **Update**.
  - If the installation is successful, the program displays a message indicating that installation is successful.
  - If the installation is not successful, click **View Log File** to troubleshoot the problem.
9. Click **Finish**.
10. Click **File > Exit** to close Installation Manager.

### Uninstalling fix packs from IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the GUI: 8.5.5.0

You can roll back IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty to an earlier version using the Installation Manager GUI.

#### Before you begin

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your computer when you install a package. If you change the default setting or delete the saved files, Installation Manager requires access to the repository that was used to install the earlier version.

#### About this task

**Note:** For information on installing and removing fix packs for WebSphere Application Server Liberty Network Deployment on distributed operating systems using the Installation Manager command line, read the following articles in this information center:

- “Installing Liberty fix packs on distributed operating systems using the command line” on page 1200
- “Uninstalling Liberty fix packs from distributed operating systems using the command line” on page 1210

#### Procedure

1. Stop all servers on the installation that is being modified.
2. Start Installation Manager.
3. Click **Roll Back**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you use to access protected IBM software websites.

4. Select the package group to roll back.
5. Click **Next**.
6. Select the version to which you want to roll back under **IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty**.
7. Click **Next**.
8. Review the summary information, and click **Roll Back**.
  - If the rollback is successful, the program displays a message indicating that the rollback is successful.

- If the rollback is not successful, click **View Log File** to troubleshoot the problem.
9. Click **Finish**.
  10. Click **File > Exit** to close Installation Manager.

### Uninstalling IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the GUI: **8.5.5.0**

Use the Installation Manager GUI to uninstall IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty.

#### Before you begin

Make sure that no commands or server profiles are using IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty before uninstalling it. Server profiles using IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty will not function if it is uninstalled.

#### Procedure

1. Log on to your system.
2. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
3. Start Installation Manager.
4. Click **Uninstall**.
5. In the **Uninstall Packages** window, perform the following actions.
  - a. Select **IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty** and the appropriate version.
  - b. Click **Next**.
6. Review the summary information.
7. Click **Uninstall**.
  - If the uninstallation is successful, the program displays a message that indicates success.
  - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
8. Click **Finish**.
9. Click **File > Exit** to close Installation Manager.

### Uninstalling IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the command line: **8.5.5.0**

You can uninstall IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using the Installation Manager command line.

#### Before you begin

Make sure that no commands or server profiles are using IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty before uninstalling it. Server profiles using IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty will not function if it is uninstalled.

#### Procedure

1. Log on to your system.
2. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
3. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
4. Use the `imcl` command to uninstall the offering.

Windows

```
imcl.exe uninstall com.ibm.websphere.liberty.IBMJAVA.v70  
-installationDirectory installation_directory
```

AIX

HP-UX

Linux

Solaris

```
./imcl uninstall com.ibm.websphere.liberty.IBMJAVA.v70  
-installationDirectory installation_directory
```

Go to the IBM Installation Manager Information Center.

## Uninstalling IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using response files: **8.5.5.0**

You can uninstall IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using Installation Manager response files.

### Before you begin

Make sure that no commands or server profiles are using IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty before uninstalling it. Server profiles using IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty will not function if it is uninstalled.

**Optional:** Perform or record the installation of Installation Manager and installation of IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty to a temporary installation registry on one of your systems so that you can use this temporary registry to record the uninstallation without using the standard registry where Installation Manager is installed.

### About this task

Using Installation Manager, you can work with response files to uninstall IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

### Procedure

1. **Optional: Record a response file to uninstall IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty:** On one of your systems, perform the following actions to record a response file that will uninstall IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty:
  - a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.
  - b. Start Installation Manager from the command line using the -record option.

For example:

- **Windows Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"  
-record C:\temp\uninstall_response_file.xml
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry  
-record /var/temp/uninstall_response_file.xml
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry  
-record user_home/var/temp/uninstall_response_file.xml
```

**Tip:** If you choose to use the -skipInstall parameter with a temporary installation registry created as described in *Before you begin*, Installation Manager uses the temporary installation registry while recording the response file. It is important to note that when the -skipInstall parameter is

specified, no packages are installed or uninstalled. All of the actions that you perform in Installation Manager simply update the installation data that is stored in the specified temporary registry. After the response file is generated, it can be used to uninstall IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty, removing the files and updating the standard installation registry.

The `-skipInstall` operation should not be used on the actual agent data location used by Installation Manager. This is unsupported. Use a clean writable location, and re-use that location for future recording sessions.

For more information, read the IBM Installation Manager Information Center.

- c. Click **Uninstall**.
  - d. In the **Uninstall Packages** window, perform the following actions.
    - 1) Select **IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty** and the appropriate version.
    - 2) Click **Next**.
  - e. Review the summary information.
  - f. Click **Uninstall**.
    - If the uninstallation is successful, the program displays a message that indicates success.
    - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
  - g. Click **Finish**.
  - h. Click **File > Exit** to close Installation Manager.
2. **Use the response file to uninstall IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty:** From a command line on each of the systems from which you want to uninstall IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager and use the response file that you created to uninstall IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty. For example:

- **Windows Administrator or non-administrator:**

```
imcl.exe
input C:\temp\uninstall_response_file.xml
-log C:\temp\uninstall_log.xml
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./imcl
input /var/temp/uninstall_response_file.xml
-log /var/temp/uninstall_log.xml
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./imcl
input user_home/var/temp/uninstall_response_file.xml
-log user_home/var/temp/uninstall_log.xml
```

Go to the IBM Installation Manager Information Center.

3. **Optional: List all installed packages to verify the uninstallation.**

**AIX HP-UX Linux Solaris**

```
./imcl listInstalledPackages
```

**Windows**

```
imcl listInstalledPackages
```

**Windows**

## Example

The following is an example of a response file for uninstalling IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty.

```

<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean='true' temporary='true'>
<uninstall modify='false'>
<offering id='com.ibm.websphere.liberty.IBMJAVA.v70'
  profile='WebSphere Liberty V8.5' />
</uninstall>
<profile id='WebSphere Liberty V8.5'
  installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
</agent-input>

```

## Installing and uninstalling SDK Java Technology Edition Version 8.0 for Liberty on distributed operating systems

8.5.5.5

You can install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using Installation Manager.

### About this task

Perform one of these procedures to install, update, roll back, or uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using Installation Manager.

You can download and install IBM WebSphere SDK Java Technology Edition Version 8.0. This version is only available from the web. This version is not available on the physical media. You have the following installation options:

- Download the installation files from the IBM Fix Central website and use a local installation.
- Access the live repositories and use your IBM Software ID for a web-based installation.

### Procedure

- Install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the GUI.
- Install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using response files.
- Install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the command line.
- Install fix packs on IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the GUI.
- Uninstall fix packs on IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the GUI.
- Uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the GUI.
- Uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using response files.
- Uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the command line.

### Results

#### Notes on logging and tracing:

- An easy way to view the logs is to open Installation Manager and go to **File > View Log**. An individual log file can be opened by selecting it in the table and then clicking the **Open log file** icon.
- Logs are located in the logs directory of Installation Manager's application data location. For example:

— **Windows** **Administrative installation:**

C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager\logs

— **Windows** **Non-administrative installation:**

C:\Documents and Settings\user\_name\Application Data\IBM\Installation Manager\logs

— **AIX** **HP-UX** **Linux** **Solaris** **Administrative installation:**

/var/ibm/InstallationManager/logs

— **AIX** **HP-UX** **Linux** **Solaris** **Non-administrative installation:**

`user_home/var/ibm/InstallationManager/logs`

- The main log files are time-stamped XML files in the logs directory, which you can view using any standard web browser.
- The `log.properties` file in the logs directory specifies the level of logging or tracing that Installation Manager uses.

### Notes on troubleshooting:

- **HP-UX** By default, some HP-UX systems are configured to not use DNS to resolve host names. This can result in Installation Manager not being able to connect to an external repository.  
You can ping the repository, but `nslookup` does not return anything.  
Work with your system administrator to configure your machine to use DNS, or use the IP address of the repository.
- For more information on using Installation Manager, read the IBM Installation Manager Information Center.  
Read the release notes to learn more about the latest version of Installation Manager. To access the release notes, complete the following task:
  - **Windows** Click **Start > Programs > IBM Installation Manager > Release Notes**.
  - **AIX** **HP-UX** **Linux** **Solaris** Go to the documentation subdirectory in the directory where Installation Manager is installed, and open the `readme.html` file.

### Installing IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the GUI:

8.5.5.5

You can install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty by using the Installation Manager GUI.

#### Before you begin

1. Prepare your system as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.
2. Install one the following offerings:
  - IBM WebSphere Application Server Liberty
  - IBM WebSphere Application Server Liberty Trial
  - IBM WebSphere Application Server Liberty Core
  - IBM WebSphere Application Server Liberty Core Trial
  - IBM WebSphere Application Server Liberty - Express
  - IBM WebSphere Application Server Liberty Network Deployment
  - IBM WebSphere Application Server Liberty Network Deployment Trial
  - IBM WebSphere Application Server Liberty for Developers
  - IBM WebSphere Application Server Liberty for Developers (ILAN)

You can download and install IBM WebSphere SDK Java Technology Edition Version 8.0. This version is only available from the web. You have the following installation options:

- Download the installation files from the IBM Fix Central website and use a local installation.
- Access the live repositories and use your IBM Software ID for a web-based installation.

**Note:** You can locate the installation files here IBM Support: Fix central .

#### Procedure

1. Start Installation Manager.

**Tip:** AIX HP-UX Linux Solaris You can start Installation Manager in group mode with the `./IBMIM` command.

- Group mode allows users to share packages in a common location and manage them with the same instance of Installation Manager.
- For more information on using group mode, read the Group mode road maps in the IBM Installation Manager Information Center.

2. Click **Install**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

Installation Manager searches its defined repositories for available packages.

3. Perform the appropriate actions.

- a. Select **IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty** and the appropriate version.

If you already have IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty installed on a WebSphere Application Server Liberty Network Deployment installation on your system, a message displays indicating that IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty is already installed. To install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty on an installation where it is not yet installed, click **Continue**.

- b. Select the fixes to install.

Any recommended fixes are selected by default.

If there are recommended fixes, you can select the option to show only recommended fixes and hide non-recommended fixes.

- c. Click **Next**.

**Note:** If you do not have and have not selected a Version 8.5 installation of one the following offerings on which to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty, an error dialog displays.

- IBM WebSphere Application Server Liberty
- IBM WebSphere Application Server Liberty Trial
- IBM WebSphere Application Server Liberty Core
- IBM WebSphere Application Server Liberty Core Trial
- IBM WebSphere Application Server Liberty - Express
- IBM WebSphere Application Server Liberty Network Deployment
- IBM WebSphere Application Server Liberty Network Deployment Trial
- IBM WebSphere Application Server Liberty for Developers
- IBM WebSphere Application Server Liberty for Developers (ILAN)

Click **OK**, select an appropriate offering on which to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty, and click **Next**.

4. Select the appropriate installation on which to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty, and click **Next**.

**Note:** The bit architecture that is installed, 32 bit or 64 bit, matches the bit selection that is made during the installation of the Liberty offering. For GUI installations of Liberty offerings, this selection is made on the Location panel. For command-line and response-file installations of Liberty offerings, the default can be overridden by using the `cic.selector.arch` property.

5. Click **Next**.

6. Review the summary information, and click **Install**.

- If the installation is successful, the program displays a message that says that installation is successful.

**Note:** The program might also display important post-installation instructions.

- If the installation is not successful, click **View Log File** to troubleshoot the problem.

7. Click **Finish**.

8. Click **File > Exit** to close Installation Manager.

### Installing IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the command line:

8.5.5.5

You can install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the Installation Manager command line.

#### Before you begin

1. Prepare your system as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.
2. Install one the following offerings:
  - IBM WebSphere Application Server Liberty
  - IBM WebSphere Application Server Liberty Trial
  - IBM WebSphere Application Server Liberty Core
  - IBM WebSphere Application Server Liberty Core Trial
  - IBM WebSphere Application Server Liberty - Express
  - IBM WebSphere Application Server Liberty Network Deployment
  - IBM WebSphere Application Server Liberty Network Deployment Trial
  - IBM WebSphere Application Server Liberty for Developers
  - IBM WebSphere Application Server Liberty for Developers (ILAN)

You can download and install IBM WebSphere SDK Java Technology Edition Version 8.0. This version is only available from the web. You have the following installation options:

- Download the installation files from the IBM Fix Central website and use a local installation.
- Access the live repositories and use your IBM Software ID for a web-based installation.

#### Procedure

1. Optional: If the repository requires a username and password, create a credential-storage file to access this repository.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the `-keyring` and `-password` options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the `-keyring` and `-password` options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

2. Log on to your system.
3. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.

#### 4. Verify that the repository is available.

Windows

```
imcl.exe listAvailablePackages -repositories path_to_repository
```

AIX

HP-UX

Linux

Solaris

```
./imcl listAvailablePackages -repositories path_to_repository
```

You should see one or more levels of the offering.

#### 5. Use the **imcl** command to install the offering.

Windows

```
imcl.exe install com.ibm.websphere.liberty.IBMJAVA.v80_offering_version  
-repositories source_repository  
-installationDirectory installation_directory  
-secureStorageFile storage_file -masterPasswordFile master_password_file
```

AIX

HP-UX

Linux

Solaris

```
./imcl install com.ibm.websphere.liberty.IBMJAVA.v80_offering_version  
-repositories source_repository  
-installationDirectory installation_directory  
-secureStorageFile storage_file -masterPasswordFile master_password_file
```

The value of the **-installationDirectory** parameter should be the location of an existing Liberty installation. The SDK offering will be installed into the `<liberty_home>\java\java_1.8_32` or `<liberty_home>\java\java_1.8_64` folder, depending on whether the installation location was configured to be 32-bit or 64-bit when the Liberty offering was initially installed.

**Note:** The bit architecture that will be installed, 32 bit or 64 bit, will match the bit selection made during the installation of the Liberty offering. For GUI installations of Liberty offerings, this selection is made on the Location panel. For command-line and response-file installations of Liberty offerings, the default can be overridden using the `cic.selector.arch` property.

#### Tips:

- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.0.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the **-installFixes** argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the **-installFixes** option defaults to all.
  - If the offering version is specified, the **-installFixes** option defaults to none.
- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lafiles` or `product_name/lafiles` subdirectory of the installation image or repository for this product.
- The program might write important post-installation instructions to standard output.

For more information on using the **imcl** command, see the IBM Installation Manager Information Center.

## Installing IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using response files:

8.5.5.5

You can install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using Installation Manager response files.

### Before you begin

1. Prepare your system as described in “Installing Installation Manager and preparing to install Liberty” on page 1168.
2. Install one the following offerings:
  - IBM WebSphere Application Server Liberty
  - IBM WebSphere Application Server Liberty Trial
  - IBM WebSphere Application Server Liberty Core
  - IBM WebSphere Application Server Liberty Core Trial
  - IBM WebSphere Application Server Liberty - Express
  - IBM WebSphere Application Server Liberty Network Deployment
  - IBM WebSphere Application Server Liberty Network Deployment Trial
  - IBM WebSphere Application Server Liberty for Developers
  - IBM WebSphere Application Server Liberty for Developers (ILAN)

### About this task

Using Installation Manager, you can work with response files to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

You can download and install IBM WebSphere SDK Java Technology Edition Version 8.0. This version and later versions are only available from the web. You have the following installation options:

- Download the installation files from the IBM Fix Central website and use a local installation.
- Access the live repositories and use your IBM Software ID for a web-based installation.

### Procedure

1. Optional: **Record a response file to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty:** On one of your systems, perform the following actions to record a response file that will install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty.
  - a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.
  - b. Start Installation Manager from the command line using the -record option.

For example:

- **Windows Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"  
-record C:\temp\install_response_file.xml
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry  
-record /var/temp/install_response_file.xml
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry  
-record user_home/var/temp/install_response_file.xml
```

**Tip:** When you record a new response file, you can specify the `-skipInstall` parameter. Using this parameter has the following benefits:

- No files are actually installed, and this speeds up the recording.
- If you use a temporary data location with the `-skipInstall` parameter, Installation Manager writes the installation registry to the specified data location while recording. When you start Installation Manager again without the `-skipInstall` parameter, you then can use your response file to install against the real installation registry.

The `-skipInstall` operation should not be used on the actual agent data location used by Installation Manager. This is unsupported. Use a clean writable location, and re-use that location for future recording sessions.

For more information, read the IBM Installation Manager Information Center.

c. Add the appropriate repositories to your Installation Manager preferences.

1) Click **File > Preferences**.

2) Select **Repositories**.

3) Perform the following actions for each repository:

a) Click **Add Repository**.

b) Enter the path to the `repository.config` file in the remote web-based repository or the local directory into which you unpacked the repository files.

For example:

- Remote repositories:

`https://downloads.mycorp.com:8080/WAS_85_repository`

or

`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v80`

- Local repositories:

– **Windows** `C:\repositories\jdk8\local-repositories`

– **AIX** **HP-UX** **Linux** **Solaris** `/var/repositories/jdk8/local-repositories`

c) Click **OK**.

4) Click **Apply**.

5) Click **OK**.

d. Click **Install**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you registered with on the program website.

Installation Manager searches its defined repositories for available packages.

e. Perform the appropriate actions.

1) Select **IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty**.

If you already have IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty installed on a WebSphere Application Server Liberty Network Deployment installation on your system in the targeted location, a message displays indicating that IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty is already installed. To install IBM WebSphere SDK Java Technology Edition Version 8.0 on a WebSphere Application Server Liberty Network Deployment installation where it is not yet installed, click **Continue**.

2) Select the fixes to install.

Any recommended fixes are selected by default.

If there are recommended fixes, you can select the option to show only recommended fixes and hide non-recommended fixes.

3) Click **Next**.

**Note:** If you do not have and have not selected an installation of one the following offerings on which to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty, an error dialog displays.

- IBM WebSphere Application Server Liberty
- IBM WebSphere Application Server Liberty Trial
- IBM WebSphere Application Server Liberty Core
- IBM WebSphere Application Server Liberty Core Trial
- IBM WebSphere Application Server Liberty - Express
- IBM WebSphere Application Server Liberty Network Deployment
- IBM WebSphere Application Server Liberty Network Deployment Trial
- IBM WebSphere Application Server Liberty for Developers
- IBM WebSphere Application Server Liberty for Developers (ILAN)

Click **OK**, select an appropriate offering on which to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty, and click **Next**.

- f. Select the appropriate WebSphere Application Server Liberty Network Deployment installation on which to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty, and click **Next**.

**Note:** The bit architecture that will be installed, 32 bit or 64 bit, will match the bit selection made during the installation of the Liberty offering. For GUI installations of Liberty offerings, this selection is made on the Location panel. For command-line and response-file installations of Liberty offerings, the default can be overridden using the `cic.selector.arch` property.

- g. Click **Next**.
- h. Review the summary information, and click **Install**.
  - If the installation is successful, the program displays a message indicating that installation is successful.

**Note:** The program might also display important post-installation instructions as well.

- If the installation is not successful, click **View Log File** to troubleshoot the problem.
- i. Click **Finish**.
- j. Click **File > Exit** to close Installation Manager.
- k. Optional: If you are using an authenticated remote repository, create a credential-storage file for silent installation.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

## 2. Use the response files to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty:

- a. Optional: **Use the response file to install the credential-storage file:** Go to a command line on each of the systems on which you want to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the credential-storage file.

For example:

- **Windows Administrator or non-administrator:**

```
imcl.exe
input C:\temp\credentialstorage_response_file.xml
-log C:\temp\credentialstorage_log.xml
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./imcl
input /var/temp/credentialstorage_response_file.xml
-log /var/temp/credentialstorage_log.xml
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./imcl
input user_home/var/temp/credentialstorage_response_file.xml
-log user_home/var/temp/credentialstorage_log.xml
```

- Use the response file to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty:** Go to a command line on each of the systems on which you want to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty, change to the eclipse/tools subdirectory in the directory where you installed Installation Manager, and install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty.

For example:

- **Windows Administrator or non-administrator:**

```
imcl.exe
input C:\temp\install_response_file.xml
-log C:\temp\install_log.xml
-secureStorageFile C:\IM\credential.store -masterPasswordFile C:\IM\master_password_file.txt
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./imcl
input /var/temp/install_response_file.xml
-log /var/temp/install_log.xml
-secureStorageFile /var/IM/credential.store -masterPasswordFile /var/IM/master_password_file.txt
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./imcl
input user_home/var/temp/install_response_file.xml
-log user_home/var/temp/install_log.xml
-secureStorageFile user_home/var/IM/credential.store -masterPasswordFile user_home/var/IM/master_password_file.txt
```

### Notes:

- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the lafiles or *product\_name/lafiles* subdirectory of the installation image or repository for this product.
- The program might write important post-installation instructions to standard output. Read the IBM Installation Manager Information Center.

### Example

**Windows** The following is an example of a response file for installing IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean="true" temporary="true">
<server>
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v80" />
</server>
<install modify='false'>
<offering id='com.ibm.websphere.liberty.IBMJAVA.v80'
profile='WebSphere Liberty V8.5' installFixes='none' />
</install>
<profile id='WebSphere Liberty V8.5' installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
</agent-input>
```

## Installing fix packs on IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the GUI: 8.5.5.5

You can update IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty to a later version using the Installation Manager GUI.

### Before you begin

Make sure that the web-based or local service repository location is listed and checked or that the **Search service repositories during installation and updates** option is selected on the Repositories panel in your Installation Manager preferences. For more information on using service repositories with Installation Manager, read the IBM Installation Manager Information Center.

### About this task

**Note:** For information on installing and removing fix packs for WebSphere Application Server Liberty Network Deployment on distributed operating systems using the Installation Manager command line, read the following articles in this information center:

- “Installing Liberty fix packs on distributed operating systems using the command line” on page 1200
- “Uninstalling Liberty fix packs from distributed operating systems using the command line” on page 1210

### Procedure

1. Start Installation Manager.
2. Click **Update**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you use to access protected IBM software websites.

3. Select the package group to update.

**Tip:** If you select **Update all**, Installation Manager will search all of the added and predefined repositories for recommended updates to all of the package groups that it has installed.

- Use this feature only if you have full control over which fixes are contained in the targeted repositories.
    - If you create and point to a set of custom repositories that include only the specific recommended fixes that you want to install, you should be able to use this feature confidently.
    - If you enable searching service repositories or install fixes directly from other live web-based repositories, you might not want to select this option so that you can select only the fixes that you want to install for each offering on subsequent panels.
  - If you select **Update all**, Installation Manager will install only the recommended updates to all of the package groups; it will not allow you to select non-recommended fixes for installation. If you want to install non-recommended fixes, perform the following actions:
    - a. On this panel, clear the **Update all** check box and select an offering to update.
    - b. On the next panel, clear the option to show only recommended fixes and then select the fixes that you want to install.
4. Click **Next**.
  5. Select the version to which you want to update under **IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty**.
  6. Click **Next**.
  7. Accept the terms in the license agreements, and click **Next**.
  8. Review the summary information, and click **Update**.

- If the installation is successful, the program displays a message indicating that installation is successful.
- If the installation is not successful, click **View Log File** to troubleshoot the problem.

9. Click **Finish**.

10. Click **File > Exit** to close Installation Manager.

### Uninstalling fix packs from IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the GUI: 8.5.5.5

You can roll back IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty to an earlier version using the Installation Manager GUI.

#### Before you begin

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your computer when you install a package. If you change the default setting or delete the saved files, Installation Manager requires access to the repository that was used to install the earlier version.

#### About this task

**Note:** For information on installing and removing fix packs for WebSphere Application Server Liberty Network Deployment on distributed operating systems using the Installation Manager command line, read the following articles in this information center:

- “Installing Liberty fix packs on distributed operating systems using the command line” on page 1200
- “Uninstalling Liberty fix packs from distributed operating systems using the command line” on page 1210

#### Procedure

1. Stop all servers on the installation that is being modified.
2. Start Installation Manager.
3. Click **Roll Back**.

**Note:** If you are prompted to authenticate, use the IBM ID and password that you use to access protected IBM software websites.

4. Select the package group to roll back.
5. Click **Next**.
6. Select the version to which you want to roll back under **IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty**.
7. Click **Next**.
8. Review the summary information, and click **Roll Back**.
  - If the rollback is successful, the program displays a message indicating that the rollback is successful.
  - If the rollback is not successful, click **View Log File** to troubleshoot the problem.
9. Click **Finish**.
10. Click **File > Exit** to close Installation Manager.

## Uninstalling IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the GUI:

8.5.5.0

Use the Installation Manager GUI to uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty.

### Before you begin

Make sure that no commands or server profiles are using IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty before uninstalling it. Server profiles using IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty will not function if it is uninstalled.

### Procedure

1. Log on to your system.
2. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
3. Start Installation Manager.
4. Click **Uninstall**.
5. In the **Uninstall Packages** window, perform the following actions.
  - a. Select **IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty** and the appropriate version.
  - b. Click **Next**.
6. Review the summary information.
7. Click **Uninstall**.
  - If the uninstallation is successful, the program displays a message that indicates success.
  - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
8. Click **Finish**.
9. Click **File > Exit** to close Installation Manager.

## Uninstalling IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the command line:

8.5.5.5

You can uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using the Installation Manager command line.

### Before you begin

Make sure that no commands or server profiles are using IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty before uninstalling it. Server profiles using IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty will not function if it is uninstalled.

### Procedure

1. Log on to your system.
2. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
3. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
4. Use the `imcl` command to uninstall the offering.

Windows

```
imcl.exe uninstall com.ibm.websphere.liberty.IBMJAVA.v80  
-installationDirectory installation_directory
```

AIX

HP-UX

Linux

Solaris

```
./imcl uninstall com.ibm.websphere.liberty.IBMJAVA.v80
-installationDirectory installation_directory
```

Go to the IBM Installation Manager Information Center.

## Uninstalling IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using response files: 8.5.5.5

You can uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty using Installation Manager response files.

### Before you begin

Make sure that no commands or server profiles are using IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty before uninstalling it. Server profiles using IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty will not function if it is uninstalled.

**Optional:** Perform or record the installation of Installation Manager and installation of IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty to a temporary installation registry on one of your systems so that you can use this temporary registry to record the uninstallation without using the standard registry where Installation Manager is installed.

### About this task

Using Installation Manager, you can work with response files to uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty in a variety of ways. You can record a response file using the GUI as described in the following procedure, or you can generate a new response file by hand or by taking an example and modifying it.

### Procedure

1. **Optional: Record a response file to uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty:** On one of your systems, perform the following actions to record a response file that will uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty:
  - a. From a command line, change to the eclipse subdirectory in the directory where you installed Installation Manager.
  - b. Start Installation Manager from the command line using the -record option.

For example:

- Windows **Administrator or non-administrator:**

```
IBMIM.exe -skipInstall "C:\temp\imRegistry"
-record C:\temp\uninstall_response_file.xml
```

- AIX HP-UX Linux Solaris **Administrator:**

```
./IBMIM -skipInstall /var/temp/imRegistry
-record /var/temp/uninstall_response_file.xml
```

- AIX HP-UX Linux Solaris **Non-administrator:**

```
./IBMIM -skipInstall user_home/var/temp/imRegistry
-record user_home/var/temp/uninstall_response_file.xml
```

**Tip:** If you choose to use the -skipInstall parameter with a temporary installation registry created as described in *Before you begin*, Installation Manager uses the temporary installation registry while recording the response file. It is important to note that when the -skipInstall parameter is specified, no packages are installed or uninstalled. All of the actions that you perform in Installation Manager simply update the installation data that is stored in the specified temporary registry. After the response file is generated, it can be used to uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty, removing the files and updating the standard installation registry.

The `-skipInstall` operation should not be used on the actual agent data location used by Installation Manager. This is unsupported. Use a clean writable location, and re-use that location for future recording sessions.

For more information, read the IBM Installation Manager Information Center.

- c. Click **Uninstall**.
  - d. In the **Uninstall Packages** window, perform the following actions.
    - 1) Select **IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty** and the appropriate version.
    - 2) Click **Next**.
  - e. Review the summary information.
  - f. Click **Uninstall**.
    - If the uninstallation is successful, the program displays a message that indicates success.
    - If the uninstallation is not successful, click **View log** to troubleshoot the problem.
  - g. Click **Finish**.
  - h. Click **File > Exit** to close Installation Manager.
2. **Use the response file to uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty:** From a command line on each of the systems from which you want to uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager and use the response file that you created to uninstall IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty. For example:

- **Windows Administrator or non-administrator:**

```
imcl.exe
input C:\temp\uninstall_response_file.xml
-log C:\temp\uninstall_log.xml
```

- **AIX HP-UX Linux Solaris Administrator:**

```
./imcl
input /var/temp/uninstall_response_file.xml
-log /var/temp/uninstall_log.xml
```

- **AIX HP-UX Linux Solaris Non-administrator:**

```
./imcl
input user_home/var/temp/uninstall_response_file.xml
-log user_home/var/temp/uninstall_log.xml
```

Go to the IBM Installation Manager Information Center.

3. **Optional: List all installed packages to verify the uninstallation.**

**AIX HP-UX Linux Solaris**

```
./imcl listInstalledPackages
```

**Windows**

```
imcl listInstalledPackages
```

**Windows**

## Example

The following is an example of a response file for uninstalling IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean='true' temporary='true'>
<uninstall modify='false'>
<offering id='com.ibm.websphere.liberty.IBMJAVA.v80'
profile='WebSphere Liberty V8.5' />
</uninstall>
```

```
<profile id='WebSphere Liberty V8.5'
  installLocation='C:\Program Files\IBM\WebSphere\Liberty'>
</profile>
</agent-input>
```

## Using the sample response files

You can edit and use sample response file for installing, modifying, or uninstalling Liberty offerings silently.

### Procedure

- “Sample response file: Installing IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty”
- “Sample response file: Uninstalling IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty” on page 1263
- “Sample response file: Installing IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty” on page 1266
- “Sample response file: Uninstalling IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty” on page 1270
- “Sample response file: Installing IBM WebSphere Application Server Liberty Network Deployment” on page 1273
- “Sample response file: Modifying IBM WebSphere Application Server Liberty Network Deployment” on page 1278
- “Sample response file: Uninstalling IBM WebSphere Application Server Liberty Network Deployment” on page 1283

### Sample response file: Installing IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty:

You can edit and use this example of a response file for installing IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty.

**Note:** 8.5.5.11 Support for using Java SE 6 with WebSphere Liberty ends in September 2017. After the end of support, the Liberty kernel will be recompiled and can no longer run with Java SE 6. If you continue to use Java SE 6 on earlier fix packs after the end of support date, you could expose your environment to security risks.

Java SE 8 is the recommended Java SDK because it provides the latest features and security updates. You can install it by installing the IBM SDK, Java Technology Edition, Version 8 package to the package group that contains WebSphere Liberty.

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright #####
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2013.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
##### -->

<!-- ##### Frequently Asked Questions #####
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
# Installation Manager Information Center can be found at:
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
```

```

#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
# Windows = IBMIM.exe -record c:\temp\responsefiles\WASv85.install.Win32.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
# Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv85.install.RHEL64.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse/tools subdirectory in the directory where you installed
# Installation Manager:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
# Windows = imcl.exe -acceptLicense -showProgress
# input c:\temp\responsefile\WASv85.install.Win32.xml
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input /home/user/responsefile/WASv85.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
# license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help: IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. There are two methods for storing authentication credentials
# for Installation Manager depending on the version being used,
# either key ring files or storage files.
#
# Versions of Installation Manger before 1.6.2 use a key ring file to store
# encrypted credentials for authenticating with repositories. Follow this
# two-step process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
# Windows = IBMIM.exe -keyring <path and file name> -password <password>
# Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
# -password <password>
#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <path and file name of response file>
# -keyring <path and name of key ring file> -password <password>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <path and file name of response file>
# -keyring <path and name of key ring file> -password <password>
#
# Versions of Installation Manager at 1.6.2 or higher use storage files
# to store encrypted credentials. Complete the following steps to create
# master password and storage files to use with Installation Manager.
#
# First, if you do not have a master password file already, create a text file
# that contains a master passphrase. An example of a passphrase is:
# "This text is the passphrase for a master password file."
#
# Next, run imutilsc under the eclipse/tools subdirectory with the following
# options to create and store user credentials in a storage file.
# -secureStorageFile <path and file name of storage file>
# -masterPasswordFile <path and file name of master password file>
# -url <repository address> or -passportAdvantage <PPA repository address>
# -userName <user name>
# -userPassword <password for user>
#
# Example of a command to create a storage file by operating system
# Windows = imutilsc saveCredential -url http://myServer -userName myUserName
# -userPassword myPassword -secureStorageFile C:\IBM\credential.store

```

```

# -masterPasswordFile C:\IBM\master_password_file.txt
# Linux, UNIX, IBM z/OS, and the OS X operating system =
# ./imutilsc saveCredential -url http://myServer -userName myUserName
# -userPassword myPassword -secureStorageFile /home/IBM/credential.store
# -masterPasswordFile /home/user/IBM/master_password_file.txt
#
# Usage hints:
# * Do not use both the -url and -passportAdvantage options in the same command.
# * Enclose file paths that include spaces with double quotation marks.
# * If you use the IBM service repositories, you can specify the value:
#   http://www.ibm.com/software/repositorymanager/entitled/repository.xml
#   for the -url option which is a generic service repository for IBM packages.
# * Repeat steps to store credentials for multiple users in one file.
# * Repeat steps to store credentials for multiple repositories in one file.
#
# Afterwards, when you start a silent installation, run imcl under the eclipse/tools
# subdirectory, and provide Installation Manager with the location of the storage
# file. For example:
#
# Windows = imcl.exe -acceptLicense -showProgress
#   input <path and file name of response file>
#   -secureStorageFile <path and name of storage file>
#   -masterPasswordFile <path and name of master password file>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#   input <path and file name of response file>
#   -secureStorageFile <path and name of storage file>
#   -masterPasswordFile <path and name of master password file>
#
##### -->

<!-- ##### Agent Input #####
#
# Note that the acceptLicense attribute has been deprecated.
# Use the -acceptLicense command line option to accept license agreements.
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
#   true = only use the repositories and other preferences that are
#         specified in the response file.
#   false = use the repositories and other preferences that are
#         specified in the response file and Installation Manager.
#
# Valid values for temporary:
#   true = repositories and other preferences specified in the
#         response file do not persist in Installation Manager.
#   false = repositories and other preferences specified in the
#         response file persist in Installation Manager.
#
##### -->

<agent-input clean="true" temporary="true">

<!-- ##### Repositories #####
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
##### -->

<server>

  <!-- ##### IBM WebSphere Live Update Repositories #####
  # These repositories contain IBMJAVA for WebSphere Application Server
  # Liberty offerings, and updates for those offerings
  #
  # To use the secure repository (https), you must have an IBM ID,
  # which can be obtained by registering at: http://www.ibm.com/account
  # or your Passport Advantage account.
  #
  # And, you must use a key ring file with your response file.
  ##### -->

  <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v60"/>

  <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

  <!-- ##### Custom Repositories #####

```

```

# Uncomment and update the repository location key below
# to specify URLs or UNC paths to any intranet repositories
# and directory paths to local repositories to use.
##### -->
<!-- <repository location='https:\w3.mycompany.com\repositories\'/> -->
<!-- <repository location='/home/user/repositories/websphere/'/> -->

<!-- ##### Local Repositories #####
# Uncomment and update the following line when using a local
# repository located on your own machine to install a
# IBMJAVA for WebSphere Application Server Liberty offering.
##### -->
<!-- <repository location='insert the full directory path inside single quotes'/'> -->

</server>

<!-- ##### Install Packages #####
#
# Install Command
#
# Use the install command to inform Installation Manager of the
# installation packages to install.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
# false = indicates not to modify an existing install by adding
# or removing features.
# true = indicates to modify an existing install by adding or
# removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for the IBM WebSphere SDK Java
# Technology Edition (Optional) .
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed at the version level specified
# as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install
# the latest version available in the repositories. The version number
# can be found in the repository.xml file in the repositories.
# For example, <offering ... version='6.0.5000.20130328_1111'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of IBMJAVA for WebSphere Application Server Liberty.
#
# IBM WebSphere SDK Java Technology Edition (Optional) 6.0.5.0 is an
# extension offering which requires a base WebSphere Application
# Server / Client product to be installed first The profile id for
# IBM WebSphere SDK Java Technology Edition (Optional) 6.0.5.0 must be
# the same as the base product.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
# none = do not install available fixes with the offering.
# recommended = installs all available recommended fixes with the offering.
# all = installs all available fixes with the offering.
#
# Interim fixes for offerings also can be installed while they
# are being installed by including the offering ID for the interim
# fix and specifying the profile ID. A commented out example is
# provided in the install command below.
#
# Installation Manager supports installing multiple offerings at once.
# Additional offerings can be included in the install command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the

```

```

# Location where the offering was installed previously.
#
# Include data keys for product specific profile properties.
# For instance, Installing IBMJAVA for Liberty Offerings on
# a 64-bit system will require to include one of the options for an IBM Software
# Development Kit, this can be specified by data key cic.selector.arch, its value
# can be either x86 (for 32-bit), or x86_64 (for 64-bit).
#
# More details for cic.selector.arch can be found in the link below:
#
# https://infocenters.hursley.ibm.com/was/vNext/draft/help/index.jsp?topic=%2Fcom.ibm.websphere.wlp.core.doc%2Fae%2Ftwlp_ins_installation_dist_silent.html
#
##### -->

<install modify="false">
<offering id="com.ibm.websphere.liberty.IBMJAVA.v60" profile="WebSphere Liberty V8.5" features="com.ibm.sdk.6" installFixes="none" />
</install>
<profile id="WebSphere Liberty V8.5" installLocation="C:\Program Files\IBM\WebSphere\Liberty">
<data key="eclipseLocation" value="C:\Program Files\IBM\WebSphere\Liberty" />
<data key="cic.selector.arch" value="x86_64" />
</profile>

<!-- ##### Shared Data Location #####
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared' />
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r5/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
# true = store downloaded artifacts in the shared data location
# false = remove downloaded artifacts from the shared data location
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
-->

<!-- ##### Preferences Settings #####
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45' />
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
<preference name='offering.service.repositories.areUsed' value='true' />

```

```

<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
-->

</agent-input>

```

## Sample response file: Uninstalling IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty:

You can edit and use this example of a response file for uninstalling IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty.

```

<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright #####
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2013.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
##### -->

<!-- ##### Frequently Asked Questions #####
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
# Installation Manager Information Center can be found at:
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
# Windows = IBMIM.exe -record c:\temp\responsefiles\WASv85.install.Win32.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
# Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv85.install.RHEL64.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
# Windows = imcl.exe -acceptLicense -showProgress
# input c:\temp\responsefile\WASv85.install.Win32.xml
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input /home/user/responsefile/WASv85.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
# license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help: IBMIM -help
#
##### -->

<!-- ##### Agent Input #####
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the uninstall finishes.
#

```

```

# Valid values for clean:
#   true = only use the repositories and other preferences that are
#         specified in the response file.
#   false = use the repositories and other preferences that are
#         specified in the response file and Installation Manager.
#
# Valid values for temporary:
#   true = repositories and other preferences specified in the
#         response file do not persist in Installation Manager.
#   false = repositories and other preferences specified in the
#         response file persist in Installation Manager.
#
##### -->
<agent-input clean="true" temporary="true">

<!-- ##### Repositories #####
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
##### -->
<!-- ##### Uninstall Packages #####
#
# Uninstall Command
#
# Use the uninstall command to inform Installation Manager of the
# installation packages to uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
#   false = indicates not to modify an existing install by adding
#         or removing features.
#   true = indicates to modify an existing install by adding or
#         removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be uninstalled. The example command below contains the
# offering ID for IBM WebSphere SDK Java Technology Edition (Optional) 6.0.5.0.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be uninstalled at the version level specified
# If the version attribute is not provided, then the default behavior is
# to uninstall the latest version. The version number can be found in
# the repository.xml file in the repositories.
# For example, <offering ... version='6.0.5000.20130328_1111'>.
#
# The profile attribute is required and must match the package group
# name for the offering to be uninstalled.
#
# The features attribute is optional. If there is no feature attribute,
# then all features are uninstalled. If features are specified, then
# only those features will be uninstalled.
# Features must be comma delimited without spaces.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# IBM WebSphere SDK Java Technology Edition (Optional) 6.0.5.0 as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, Installing WebSphere Application Server Liberty Offerings on
# a 64-bit system will require to include one of the options for an IBM Software
# Development Kit, this can be specified by data key cic.selector.arch, its value
# can be either x86 (for 32-bit), or x86_64 (for 64-bit).
#
# More details for cic.selector.arch can be found in the link below:
#
# https://infocenters.hursley.ibm.com/was/vNext/draft/help/index.jsp?topic=%2Fcom.ibm.websphere.wlp.core.doc%2Fae%2Ftwlp_ins_installation_dist_silent.html
#

```

```

##### -->

<uninstall modify="false">
<offering id="com.ibm.websphere.liberty.IBMJAVA.v60" profile="WebSphere Liberty V8.5" features="com.ibm.sdk.6" />
</uninstall>
<profile id="WebSphere Liberty V8.5" installLocation="C:\Program Files\IBM\WebSphere\Liberty">
<data key="eclipseLocation" value="C:\Program Files\IBM\WebSphere\Liberty" />
<data key="cic.selector.arch" value="x86_64" />
</profile>

<!-- ##### Shared Data Location #####
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared' />
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r5/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#   true = store downloaded artifacts in the shared data location
#   false = remove downloaded artifacts from the shared data location
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
-->

<!-- ##### Preferences Settings #####
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45' />
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
<preference name='offering.service.repositories.areUsed' value='true' />
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
<preference name='http.ntlm.auth.kind' value='NTLM' />
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
<preference name='PassportAdvantageIsEnabled' value='false' />
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false' />
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true' />
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true' />

```

```
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true' />
-->

</agent-input>
```

## Sample response file: Installing IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty:

You can edit and use this example of a response file for installing IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty.

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright #####
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2013.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
##### -->

<!-- ##### Frequently Asked Questions #####
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
# Installation Manager Information Center can be found at:
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
# Windows = IBMIM.exe -record c:\temp\responsefiles\WASv85.install.Win32.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
# Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv85.install.RHEL64.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
# Windows = imcl.exe -acceptLicense -showProgress
# input c:\temp\responsefile\WASv85.install.Win32.xml
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input /home/user/responsefile/WASv85.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
# license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help: IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. There are two methods for storing authentication credentials
# for Installation Manager depending on the version being used,
# either key ring files or storage files.
#
# Versions of Installation Manger before 1.6.2 use a key ring file to store
# encrypted credentials for authenticating with repositories. Follow this
# two-step process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
# Windows = IBMIM.exe -keyring <path and file name> -password <password>
# Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
# -password <password>
```

```

#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
# Windows = imcl.exe -acceptLicense -showProgress
#   input <path and file name of response file>
#   -keyring <path and name of key ring file> -password <password>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#   input <path and file name of response file>
#   -keyring <path and name of key ring file> -password <password>
#
# Versions of Installation Manager at 1.6.2 or higher use storage files
# to store encrypted credentials. Complete the following steps to create
# master password and storage files to use with Installation Manager.
#
# First, if you do not have a master password file already, create a text file
# that contains a master passphrase. An example of a passphrase is:
# "This text is the passphrase for a master password file."
#
# Next, run imutilsc under the eclipse/tools subdirectory with the following
# options to create and store user credentials in a storage file.
# -secureStorageFile <path and file name of storage file>
# -masterPasswordFile <path and file name of master password file>
# -url <repository address> or -passportAdvantage <PPA repository address>
# -userName <user name>
# -userPassword <password for user>
#
# Example of a command to create a storage file by operating system
# Windows = imutilsc saveCredential -url http://myServer -userName myUserName
#   -userPassword myPassword -secureStorageFile C:\IBM\credential.store
#   -masterPasswordFile C:\IBM\master_password_file.txt
# Linux, UNIX, IBM z/OS, and the OS X operating system =
# ./imutilsc saveCredential -url http://myServer -userName myUserName
#   -userPassword myPassword -secureStorageFile /home/IBM/credential.store
#   -masterPasswordFile /home/user/IBM/master_password_file.txt
#
# Usage hints:
# * Do not use both the -url and -passportAdvantage options in the same command.
# * Enclose file paths that include spaces with double quotation marks.
# * If you use the IBM service repositories, you can specify the value:
#   http://www.ibm.com/software/repositorymanager/entitled/repository.xml
#   for the -url option which is a generic service repository for IBM packages.
# * Repeat steps to store credentials for multiple users in one file.
# * Repeat steps to store credentials for multiple repositories in one file.
#
# Afterwards, when you start a silent installation, run imcl under the eclipse/tools
# subdirectory, and provide Installation Manager with the location of the storage
# file. For example:
#
# Windows = imcl.exe -acceptLicense -showProgress
#   input <path and file name of response file>
#   -secureStorageFile <path and name of storage file>
#   -masterPasswordFile <path and name of master password file>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#   input <path and file name of response file>
#   -secureStorageFile <path and name of storage file>
#   -masterPasswordFile <path and name of master password file>
#
##### -->
<!-- ##### Agent Input #####
#
# Note that the acceptLicense attribute has been deprecated.
# Use the -acceptLicense command line option to accept license agreements.
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
#   true = only use the repositories and other preferences that are
#         specified in the response file.
#   false = use the repositories and other preferences that are
#         specified in the response file and Installation Manager.
#
# Valid values for temporary:
#   true = repositories and other preferences specified in the
#         response file do not persist in Installation Manager.
#   false = repositories and other preferences specified in the

```

```

#           response file persist in Installation Manager.
#
##### -->
<agent-input clean="true" temporary="true">

<!-- ##### Repositories #####
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
##### -->

<server>

  <!-- ##### IBM WebSphere Live Update Repositories #####
  # These repositories contain IBMJAVA for WebSphere Application Server
  # Liberty offerings, and updates for those offerings
  #
  # To use the secure repository (https), you must have an IBM ID,
  # which can be obtained by registering at: http://www.ibm.com/account
  # or your Passport Advantage account.
  #
  # And, you must use a key ring file with your response file.
  ##### -->

  <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v70"/>

  <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

  <!-- ##### Custom Repositories #####
  # Uncomment and update the repository location key below
  # to specify URLs or UNC paths to any intranet repositories
  # and directory paths to local repositories to use.
  ##### -->
  <!-- <repository location='https:\w3.mycompany.com\repositories\' /> -->
  <!-- <repository location='/home/user/repositories/websphere/' /> -->

  <!-- ##### Local Repositories #####
  # Uncomment and update the following line when using a local
  # repository located on your own machine to install a
  # IBMJAVA for WebSphere Application Server Liberty offering.
  ##### -->
  <!-- <repository location='insert the full directory path inside single quotes' /> -->

</server>

<!-- ##### Install Packages #####
#
# Install Command
#
# Use the install command to inform Installation Manager of the
# installation packages to install.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
# false = indicates not to modify an existing install by adding
#         or removing features.
# true = indicates to modify an existing install by adding or
#        removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for the IBM WebSphere SDK Java
# Technology Edition (Optional) .
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed at the version level specified
# as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install
# the latest version available in the repositories. The version number
# can be found in the repository.xml file in the repositories.
# For example, <offering ... version='7.0.4000.20130328_1111'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of IBMJAVA for WebSphere Application Server Liberty.

```

```

#
# IBM WebSphere SDK Java Technology Edition (Optional) 7.0.4.0 is an
# extension offering which requires a base WebSphere Application
# Server / Client product to be installed first The profile id for
# IBM WebSphere SDK Java Technology Edition (Optional) 7.0.4.0 must be
# the same as the base product.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
#   none = do not install available fixes with the offering.
#   recommended = installs all available recommended fixes with the offering.
#   all = installs all available fixes with the offering.
#
# Interim fixes for offerings also can be installed while they
# are being installed by including the offering ID for the interim
# fix and specifying the profile ID. A commented out example is
# provided in the install command below.
#
# Installation Manager supports installing multiple offerings at once.
# Additional offerings can be included in the install command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# Include data keys for product specific profile properties.
# For instance, Installing IBMJAVA for Liberty Offerings on
# a 64-bit system will require to include one of the options for an IBM Software
# Development Kit, this can be specified by data key cic.selector.arch, its value
# can be either x86 (for 32-bit), or x86_64 (for 64-bit).
#
# More details for cic.selector.arch can be found in the link below:
#
# https://infocenters.hursley.ibm.com/was/vNext/draft/help/index.jsp?topic=%2Fcom.ibm.websphere.wlp.core.doc%2Fae%2Ftwlp_ins_installation_dist_silent.html
##### -->

<install modify="false">
<offering id="com.ibm.websphere.liberty.IBMJAVA.v70" profile="WebSphere Liberty V8.5" features="com.ibm.sdk.7" installFixes="none" />
</install>
<profile id="WebSphere Liberty V8.5" installLocation="C:\Program Files\IBM\WebSphere\Liberty">
<data key="eclipseLocation" value="C:\Program Files\IBM\WebSphere\Liberty" />
<data key="cic.selector.arch" value="x86_64" />
</profile>

<!-- ##### Shared Data Location #####
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared' />
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r5/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than

```

```

# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#   true = store downloaded artifacts in the shared data location
#   false = remove downloaded artifacts from the shared data location
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
-->

<!-- ##### Preferences Settings #####
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
-->

</agent-input>

```

## Sample response file: Uninstalling IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty:

You can edit and use this example of a response file for uninstalling IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty.

```

<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright #####
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2013.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
##### -->

<!-- ##### Frequently Asked Questions #####
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
# Installation Manager Information Center can be found at:
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do

```

```

# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
# Windows = IBMIM.exe -record c:\temp\responsefiles\WASv85.install.Win32.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
# Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv85.install.RHEL64.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
# Windows = imcl.exe -acceptLicense -showProgress
# input c:\temp\responsefile\WASv85.install.Win32.xml
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input /home/user/responsefile/WASv85.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
# license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help: IBMIM -help
#
##### -->

<!-- ##### Agent Input #####
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the uninstall finishes.
#
# Valid values for clean:
# true = only use the repositories and other preferences that are
# specified in the response file.
# false = use the repositories and other preferences that are
# specified in the response file and Installation Manager.
#
# Valid values for temporary:
# true = repositories and other preferences specified in the
# response file do not persist in Installation Manager.
# false = repositories and other preferences specified in the
# response file persist in Installation Manager.
#
##### -->

<agent-input clean="true" temporary="true">

<!-- ##### Repositories #####
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
##### -->

<!-- ##### Uninstall Packages #####
#
# Uninstall Command
#
# Use the uninstall command to inform Installation Manager of the
# installation packages to uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
# false = indicates not to modify an existing install by adding
# or removing features.
# true = indicates to modify an existing install by adding or
# removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be uninstalled. The example command below contains the

```

```

# offering ID for IBM WebSphere SDK Java Technology Edition (Optional) 7.0.4.0.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be uninstalled at the version level specified
# If the version attribute is not provided, then the default behavior is
# to uninstall the latest version. The version number can be found in
# the repository.xml file in the repositories.
# For example, <offering ... version='7.0.4000.20130328_1111'>.
#
# The profile attribute is required and must match the package group
# name for the offering to be uninstalled.
#
# The features attribute is optional. If there is no feature attribute,
# then all features are uninstalled. If features are specified, then
# only those features will be uninstalled.
# Features must be comma delimited without spaces.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# IBM WebSphere SDK Java Technology Edition (Optional) 7.0.4.0 as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, Installing WebSphere Application Server Liberty Offerings on
# a 64-bit system will require to include one of the options for an IBM Software
# Development Kit, this can be specified by data key cic.selector.arch, its value
# can be either x86 (for 32-bit), or x86_64 (for 64-bit).
#
# More details for cic.selector.arch can be found in the link below:
#
# https://infocenters.hursley.ibm.com/was/vNext/draft/help/index.jsp?topic=%2Fcom.ibm.websphere.wlp.core.doc%2Fae%2Ftwlp_ins_installation_dist_silent.html
#
##### -->

<uninstall modify="false">
<offering id="com.ibm.websphere.liberty.IBMJAVA.v70" profile="WebSphere Liberty V8.5" features="com.ibm.sdk.7" />
</uninstall>
<profile id="WebSphere Liberty V8.5" installLocation="C:\Program Files\IBM\WebSphere\Liberty">
<data key="eclipseLocation" value="C:\Program Files\IBM\WebSphere\Liberty" />
<data key="cic.selector.arch" value="x86_64" />
</profile>

<!-- ##### Shared Data Location #####
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared' />
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r5/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
# true = store downloaded artifacts in the shared data location
# false = remove downloaded artifacts from the shared data location
#
##### -->

```

```

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared'>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'>
-->

<!-- ##### Preferences Settings #####
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'>
<preference name='offering.service.repositories.areUsed' value='true'>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'>
<preference name='http.ntlm.auth.kind' value='NTLM'>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'>
<preference name='PassportAdvantageIsEnabled' value='false'>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'>
-->

</agent-input>

```

## Sample response file: Installing IBM WebSphere Application Server Liberty Network Deployment:

You can edit and use this example of a response file for installing IBM WebSphere Application Server Liberty Network Deployment.

**Note:** 8.5.5.5 For Version 8.5.5.5 and later, `user.accept.license=true` is not required.

```

<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright #####
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2013.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
##### -->

<!-- ##### Frequently Asked Questions #####
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
# Installation Manager Information Center can be found at:
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
# Windows = IBMIM.exe -record c:\temp\responsefiles\WASv85.install.Win32.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry

```

```

# Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv85.install.RHEL64.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
# Windows = imcl.exe -acceptLicense -showProgress
# input c:\temp\responsefile\WASv85.install.Win32.xml
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input /home/user/responsefile/WASv85.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
# license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help: IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. There are two methods for storing authentication credentials
# for Installation Manager depending on the version being used,
# either key ring files or storage files.
#
# Versions of Installation Manager before 1.6.2 use a key ring file to store
# encrypted credentials for authenticating with repositories. Follow this
# two-step process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
# Windows = IBMIM.exe -keyring <path and file name> -password <password>
# Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
# -password <password>
#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <path and file name of response file>
# -keyring <path and name of key ring file> -password <password>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <path and file name of response file>
# -keyring <path and name of key ring file> -password <password>
#
# Versions of Installation Manager at 1.6.2 or higher use storage files
# to store encrypted credentials. Complete the following steps to create
# master password and storage files to use with Installation Manager.
#
# First, if you do not have a master password file already, create a text file
# that contains a master passphrase. An example of a passphrase is:
# "This text is the passphrase for a master password file."
#
# Next, run imutilsc under the eclipse/tools subdirectory with the following
# options to create and store user credentials in a storage file.
# -secureStorageFile <path and file name of storage file>
# -masterPasswordFile <path and file name of master password file>
# -url <repository address> or -passportAdvantage <PPA repository address>
# -userName <user name>
# -userPassword <password for user>
#
# Example of a command to create a storage file by operating system
# Windows = imutilsc saveCredential -url http://myServer -userName myUserName
# -userPassword myPassword -secureStorageFile C:\IBM\credential.store
# -masterPasswordFile C:\IBM\master_password_file.txt
# Linux, UNIX, IBM z/OS, and the OS X operating system =
# ./imutilsc saveCredential -url http://myServer -userName myUserName
# -userPassword myPassword -secureStorageFile /home/IBM/credential.store
# -masterPasswordFile /home/user/IBM/master_password_file.txt
#
# Usage hints:

```

```

# * Do not use both the -url and -passportAdvantage options in the same command.
# * Enclose file paths that include spaces with double quotation marks.
# * If you use the IBM service repositories, you can specify the value:
#   http://www.ibm.com/software/repositorymanager/entitled/repository.xml
#   for the -url option which is a generic service repository for IBM packages.
# * Repeat steps to store credentials for multiple users in one file.
# * Repeat steps to store credentials for multiple repositories in one file.
#
# Afterwards, when you start a silent installation, run imcl under the eclipse/tools
# subdirectory, and provide Installation Manager with the location of the storage
# file. For example:
#
# Windows = imcl.exe -acceptLicense -showProgress
#   input <path and file name of response file>
#   -secureStorageFile <path and name of storage file>
#   -masterPasswordFile <path and name of master password file>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#   input <path and file name of response file>
#   -secureStorageFile <path and name of storage file>
#   -masterPasswordFile <path and name of master password file>
#
##### -->

<!-- ##### Agent Input #####
#
# Note that the acceptLicense attribute has been deprecated.
# Use the -acceptLicense command line option to accept license agreements.
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
#   true = only use the repositories and other preferences that are
#         specified in the response file.
#   false = use the repositories and other preferences that are
#          specified in the response file and Installation Manager.
#
# Valid values for temporary:
#   true = repositories and other preferences specified in the
#         response file do not persist in Installation Manager.
#   false = repositories and other preferences specified in the
#         response file persist in Installation Manager.
#
##### -->

<agent-input clean="true" temporary="true">

<!-- ##### Repositories #####
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
##### -->

<server>
  <!-- ##### IBM WebSphere Live Update Repositories #####
  # These repositories contain WebSphere Application Server Liberty offerings,
  # and updates for those offerings
  #
  # To use the secure repository (https), you must have an IBM ID,
  # which can be obtained by registering at: http://www.ibm.com/account
  # or your Passport Advantage account.
  #
  # And, you must use a key ring file with your response file.
  ##### -->
  <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85"/>
  <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

  <!-- ##### Custom Repositories #####
  # Uncomment and update the repository location key below
  # to specify URLs or UNC paths to any intranet repositories
  # and directory paths to local repositories to use.
  ##### -->
  <!-- <repository location='https:\\w3.mycompany.com\repositories\' /> -->
  <!-- <repository location='/home/user/repositories/websphere/' /> -->

  <!-- ##### Local Repositories #####
  # Uncomment and update the following line when using a local
  # repository located on your own machine to install a

```

```

# WebSphere Application Server Liberty offering.
##### -->
<!-- <repository location='insert the full directory path inside single quotes' /> -->
</server>

<!-- ##### Install Packages #####
#
# Install Command
#
# Use the install command to inform Installation Manager of the
# installation packages to install.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
# false = indicates not to modify an existing install by adding
# or removing features.
# true = indicates to modify an existing install by adding or
# removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for the Network Deployment
# edition of WebSphere Application Server Liberty.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed at the version level specified
# as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install
# the latest version available in the repositories. The version number
# can be found in the repository.xml file in the repositories.
# For example, <offering ... version='8.5.5000.20130326_0211'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of WebSphere Application Server Liberty.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Application Server Liberty include:
# liberty,embeddablecontainer,extprogmodels
#
# The features embeddablecontainer,extprogmodels
# are subfeatures of liberty.
#
# You can use these functions to add or remove feature embeddablecontainer or extprogmodels later.
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
# none = do not install available fixes with the offering.
# recommended = installs all available recommended fixes with the offering.
# all = installs all available fixes with the offering.
#
# Interim fixes for offerings also can be installed while they
# are being installed by including the offering ID for the interim
# fix and specifying the profile ID.
#
# Installation Manager supports installing multiple offerings at once.
# Additional offerings can be included in the install command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# WebSphere Application Server Liberty as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, installing a WebSphere Application Server Liberty offering
# on a 64-bit system requires including the data key cic.selector.arch
# with either the value x86 (for 32-bit) or x86_64 (for 64-bit) for
# the IBM WebSphere Software Development Kit Java Technology Edition.

```

```

#
# More details for cic.selector.arch can be found in the link below:
# http://www14.software.ibm.com/webapp/wsbroker/redirect?version=phil&product=was-nd-mp&topic=twlp_ins_installation_dist_silent
#
# Two optional data keys were introduced for WebSphere Application Server Liberty
# offerings in version 8.5.5.2 that enable installing additional product assets
# during an installation or update.
#
# <data key='user.feature' value='FeatureA,FeatureB' />
# <data key='user.accept.license' value='true' />
#
# Use the user.feature data key to specify the names of one or more assets to install.
# Separate multiple assets names with a comma.
#
# For Liberty version 8.5.5.2, the available assets are:
# com.ibm.websphere.appserver.adminCenter-1.0 - The adminCenter-1.0 feature is a web-based
# graphical interface for managing Liberty servers and applications and other
# resources from a web browser on a cell phone, tablet, or computer.
#
# com.ibm.websphere.appserver.jca-1.6 - This feature enables the configuration of resource
# adapters to access Enterprise Information Systems (EIS) from applications. The
# configuration of a resource adapter also includes the configuration of connection
# factories, administered objects and activation specifications. Any resource adapter
# that complies with the JCA 1.0 specification can be used. High performance connection
# pooling is also provided.
#
# com.ibm.websphere.appserver.jcaInboundSecurity-1.0 - This feature enables security inflow for resource adapters.
#
# com.ibm.websphere.appserver.jms-1.1 - This feature enables the configuration of resource
# adapters to access messaging systems using the Java Message Service API. This also
# includes the configuration JMS connection factories, queues, topics and activation
# specifications. Any JMS resource adapter that complies with the JCA 1.6 specification
# can be used.
#
# com.ibm.websphere.appserver.mdb-3.1 - This feature enables the use of Message-Driven Enterprise
# JavaBeans. MDBs allow asynchronous processing of messages within a Java EE component.
#
# A current list of the assets available for installation is maintained in the following article.
# http://www14.software.ibm.com/webapp/wsbroker/redirect?version=phil&product=was-nd-mp&topic=twlp_ins_installation_dist_silent
#
# The user.accept.license data key is required and its value must be true,
# to indicate acceptance of the licenses for the assets or acknowledge they
# are governed by the terms of the license agreement of the product offering,
# if any additional assets are being installed.
##### -->

<install modify="false">
<offering id="com.ibm.websphere.liberty.ND.v85" profile="WebSphere Liberty V8.5" features="liberty,embeddablecontainer,extprogmodels" installFixes="none" />
</install>
<profile id="WebSphere Liberty V8.5" installLocation="C:\Program Files\IBM\WebSphere\Liberty">
<data key="eclipseLocation" value="C:\Program Files\IBM\WebSphere\Liberty" />
<data key="cic.selector.arch" value="x86_64" />
</profile>

<!-- ##### Shared Data Location #####
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared' />
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r5/index.jsp?topic=/com.ibm.silentinstall112.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
# true = store downloaded artifacts in the shared data location

```

```

# false = remove downloaded artifacts from the shared data location
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
-->

<!-- ##### Preferences Settings #####
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45' />
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
<preference name='offering.service.repositories.areUsed' value='true' />
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
<preference name='http.ntlm.auth.kind' value='NTLM' />
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
<preference name='PassportAdvantageIsEnabled' value='false' />
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false' />
-->

</agent-input>

```

## Sample response file: Modifying IBM WebSphere Application Server Liberty Network Deployment:

You can edit and use this example of a response file for modifying IBM WebSphere Application Server Liberty Network Deployment.

```

<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright #####
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2013.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
##### -->

<!-- ##### Frequently Asked Questions #####
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
# Installation Manager Information Center can be found at:
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
# Windows = IBMIM.exe -record c:\temp\responsefiles\WASv85.install.Win32.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
# Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv85.install.RHEL64.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?

```

```

# Answer 2. Create a silent installation response file and run the following command
# from the eclipse/tools subdirectory in the directory where you installed
# Installation Manager:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#   input <response_file_path_and_name> -log <log_file_path_and_name>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#   input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
#   Windows = imcl.exe -acceptLicense -showProgress
#   input c:\temp\responsefile\WASv85.install.Win32.xml
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#   input /home/user/responsefile/WASv85.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
# license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help: IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. There are two methods for storing authentication credentials
# for Installation Manager depending on the version being used,
# either key ring files or storage files.
#
# Versions of Installation Manger before 1.6.2 use a key ring file to store
# encrypted credentials for authenticating with repositories. Follow this
# two-step process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
#   Windows = IBMIM.exe -keyring <path and file name> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
#   -password <password>
#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
#   Windows = imcl.exe -acceptLicense -showProgress
#   input <path and file name of response file>
#   -keyring <path and name of key ring file> -password <password>
#   Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
#   input <path and file name of response file>
#   -keyring <path and name of key ring file> -password <password>
#
# Versions of Installation Manager at 1.6.2 or higher use storage files
# to store encrypted credentials. Complete the following steps to create
# master password and storage files to use with Installation Manager.
#
# First, if you do not have a master password file already, create a text file
# that contains a master passphrase. An example of a passphrase is:
# "This text is the passphrase for a master password file."
#
# Next, run imutilsc under the eclipse/tools subdirectory with the following
# options to create and store user credentials in a storage file.
# -secureStorageFile <path and file name of storage file>
# -masterPasswordFile <path and file name of master password file>
# -url <repository address> or -passportAdvantage <PPA repository address>
# -userName <user name>
# -userPassword <password for user>
#
# Example of a command to create a storage file by operating system
# Windows = imutilsc saveCredential -url http://myServer -userName myUserName
# -userPassword myPassword -secureStorageFile C:\IBM\credential.store
# -masterPasswordFile C:\IBM\master_password_file.txt
# Linux, UNIX, IBM z/OS, and the OS X operating system =
# ./imutilsc saveCredential -url http://myServer -userName myUserName
# -userPassword myPassword -secureStorageFile /home/IBM/credential.store
# -masterPasswordFile /home/user/IBM/master_password_file.txt
#
# Usage hints:
# * Do not use both the -url and -passportAdvantage options in the same command.
# * Enclose file paths that include spaces with double quotation marks.
# * If you use the IBM service repositories, you can specify the value:
#   http://www.ibm.com/software/repositorymanager/entitled/repository.xml

```

```

# for the -url option which is a generic service repository for IBM packages.
# * Repeat steps to store credentials for multiple users in one file.
# * Repeat steps to store credentials for multiple repositories in one file.
#
# Afterwards, when you start a silent installation, run imcl under the eclipse/tools
# subdirectory, and provide Installation Manager with the location of the storage
# file. For example:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <path and file name of response file>
# -secureStorageFile <path and name of storage file>
# -masterPasswordFile <path and name of master password file>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <path and file name of response file>
# -secureStorageFile <path and name of storage file>
# -masterPasswordFile <path and name of master password file>
#
##### -->

<!-- ##### Agent Input #####
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
# true = only use the repositories and other preferences that are
# specified in the response file.
# false = use the repositories and other preferences that are
# specified in the response file and Installation Manager.
#
# Valid values for temporary:
# true = repositories and other preferences specified in the
# response file do not persist in Installation Manager.
# false = repositories and other preferences specified in the
# response file persist in Installation Manager.
#
##### -->

<agent-input clean="true" temporary="true">

<!-- ##### Repositories #####
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
##### -->

<server>
  <!-- ##### IBM WebSphere Live Update Repositories #####
  # These repositories contain WebSphere Application Server Liberty offerings,
  # and updates for those offerings
  #
  # To use the secure repository (https), you must have an IBM ID,
  # which can be obtained by registering at: http://www.ibm.com/account
  # or your Passport Advantage account.
  #
  # And, you must use a key ring file with your response file.
  ##### -->
  <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85"/>
  <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

  <!-- ##### Custom Repositories #####
  # Uncomment and update the repository location key below
  # to specify URLs or UNC paths to any intranet repositories
  # and directory paths to local repositories to use.
  ##### -->
  <!-- <repository location='https://w3.mycompany.com/repositories/' /> -->
  <!-- <repository location='/home/user/repositories/websphere/' /> -->

  <!-- ##### Local Repositories #####
  # Uncomment and update the following line when using a local
  # repository located on your own machine to install a
  # WebSphere Application Server Liberty offering.
  ##### -->
  <!-- <repository location='insert the full directory path inside single quotes' /> -->
</server>

<!-- ##### Modify Packages #####
#

```

```

# Install and Uninstall Commands
#
# Use the install and uninstall commands to inform Installation Manager
# of the installation packages to install or uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
#   false = indicates not to modify an existing install by adding
#           or removing features.
#   true  = indicates to modify an existing install by adding or
#           removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for the Network Deployment
# edition of WebSphere Application Server Liberty.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed or uninstalled at the version level
# specified as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install or
# uninstall the latest version available in the repositories. The version
# number can be found in the repository.xml file in the repositories.
# For example, <offering ... version='8.5.5000.20130328_1111'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of WebSphere Application Server Liberty.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Application Server Liberty include:
# liberty,embeddablecontainer,extprogmodels
#
# The features embeddablecontainer,extprogmodels
# are subfeatures of liberty.
#
# You can use these functions to add or remove feature embeddablecontainer
# or extprogmodels later.
#
# In the example that follows, the feature embeddablecontainer and extprogmodels
# are being added and no feature are being removed from the specified offering.
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
#   none = do not install available fixes with the offering.
#   recommended = installs all available recommended fixes with the offering.
#   all = installs all available fixes with the offering.
#
# Installation Manager supports modifying multiple offerings at once.
# Additional offerings can be included in the install and uninstall commands,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# WebSphere Application Server Liberty as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, Installing WebSphere Application Server Liberty Offerings on
# a 64-bit system will require to include one of the options for an IBM Software
# Development Kit, this can be specified by data key cic.selector.arch, its value
# can be either x86 (for 32-bit), or x86_64 (for 64-bit).
#
# More details for cic.selector.arch can be found in the link below:
#
# https://infocenters.hursley.ibm.com/was/vNext/draft/help/index.jsp?topic=%2Fcom.ibm.websphere.wlp.core.doc%2Fae%2Ftwlp_ins_installation_dist_silent.html
#
##### -->

```

```

<install modify="true">
<offering id="com.ibm.websphere.liberty.ND.v85" profile="WebSphere Liberty V8.5" features="embeddablecontainer,extprogmodels" />
</install>
<profile id="WebSphere Liberty V8.5" installLocation="C:\Program Files\IBM\WebSphere\Liberty">
<data key="eclipseLocation" value="C:\Program Files\IBM\WebSphere\Liberty" />
<data key="cic.selector.arch" value="x86_64" />
</profile>

<!-- ##### Shared Data Location #####
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared' />
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r5/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
# true = store downloaded artifacts in the shared data location
# false = remove downloaded artifacts from the shared data location
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
-->

<!-- ##### Preferences Settings #####
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45' />
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
<preference name='offering.service.repositories.areUsed' value='true' />
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
<preference name='http.ntlm.auth.kind' value='NTLM' />
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
<preference name='PassportAdvantageIsEnabled' value='false' />
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false' />
-->

</agent-input>

```

## Sample response file: Uninstalling IBM WebSphere Application Server Liberty Network Deployment:

You can edit and use this example of a response file for uninstalling IBM WebSphere Application Server Liberty Network Deployment.

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright #####
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2013.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
##### -->

<!-- ##### Frequently Asked Questions #####
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
# Installation Manager Information Center can be found at:
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
# Windows = IBMIM.exe -record c:\temp\responsefiles\WASv85.install.Win32.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
# Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv85.install.RHEL64.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
# Windows = imcl.exe -acceptLicense -showProgress
# input c:\temp\responsefile\WASv85.install.Win32.xml
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input /home/user/responsefile/WASv85.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
# license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help: IBMIM -help
#
##### -->

<!-- ##### Agent Input #####
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the uninstall finishes.
#
# Valid values for clean:
# true = only use the repositories and other preferences that are
# specified in the response file.
# false = use the repositories and other preferences that are
# specified in the response file and Installation Manager.
#
# Valid values for temporary:
# true = repositories and other preferences specified in the
# response file do not persist in Installation Manager.
# false = repositories and other preferences specified in the
# response file persist in Installation Manager.
#
##### -->

<agent-input clean="true" temporary="true">

<!-- ##### Repositories #####
# Repositories are locations that Installation Manager queries for
```

```

# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
##### -->

<server>
<!-- ##### IBM WebSphere Live Update Repositories #####
# These repositories contain WebSphere Application Server Liberty offerings,
# and updates for those offerings
#
# To use the secure repository (https), you must have an IBM ID,
# which can be obtained by registering at: http://www.ibm.com/account
# or your Passport Advantage account.
#
# And, you must use a key ring file with your response file.
##### -->
<!--repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85"/-->
<!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

<!-- ##### Custom Repositories #####
# Uncomment and update the repository location key below
# to specify URLs or UNC paths to any intranet repositories
# and directory paths to local repositories to use.
##### -->
<!-- <repository location='https:\w3.mycompany.com\repositories\' /> -->
<!-- <repository location='/home/user/repositories/websphere/' /> -->

<!-- ##### Local Repositories #####
# Uncomment and update the following line when using a local
# repository located on your own machine to install a
# WebSphere Application Server Liberty offering.
##### -->
<!-- <repository location='insert the full directory path inside single quotes' /> -->
</server>

<!-- ##### Uninstall Packages #####
#
# Uninstall Command
#
# Use the uninstall command to inform Installation Manager of the
# installation packages to uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
# false = indicates not to modify an existing install by adding
# or removing features.
# true = indicates to modify an existing install by adding or
# removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be uninstalled. The example command below contains the
# offering ID for WebSphere Application Server Liberty Network Deployment edition.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be uninstalled at the version level specified
# If the version attribute is not provided, then the default behavior is
# to uninstall the latest version. The version number can be found in
# the repository.xml file in the repositories.
# For example, <offering ... version='8.5.5000.20130326_0211'>.
#
# The profile attribute is required and must match the package group
# name for the offering to be uninstalled.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Application Server Liberty include:
# liberty,embeddablecontainer,extprogmodels
#
# The features embeddablecontainer,extprogmodels
# are subfeatures of liberty.
#
# Installation Manager supports uninstalling multiple offerings at once.
# Additional offerings can be included in the uninstall command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.

```

```

#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# WebSphere Application Server Liberty as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, Installing WebSphere Application Server Liberty Offerings on
# a 64-bit system will require to include one of the options for an IBM Software
# Development Kit, this can be specified by data key cic.selector.arch, its value
# can be either x86 (for 32-bit), or x86_64 (for 64-bit).
#
# More details for cic.selector.arch can be found in the link below:
#
# https://infocenters.hursley.ibm.com/was/vNext/draft/help/index.jsp?topic=%2Fcom.ibm.websphere.wlp.core.doc%2Fae%2Ftwlp_ins_installation_dist_silent.html
#
##### -->

<uninstall modify="false">
<offering id="com.ibm.websphere.liberty.ND.v85" profile="WebSphere Liberty V8.5" features="liberty,embeddablecontainer,extprogmodels" />
</uninstall>
<profile id="WebSphere Liberty V8.5" installLocation="C:\Program Files\IBM\WebSphere\Liberty">
<data key="eclipseLocation" value="C:\Program Files\IBM\WebSphere\Liberty" />
<data key="cic.selector.arch" value="x86_64" />
</profile>

<!-- ##### Shared Data Location #####
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared' />
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r5/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
# true = store downloaded artifacts in the shared data location
# false = remove downloaded artifacts from the shared data location
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
-->

<!-- ##### Preferences Settings #####
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of

```

```

# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
-->

</agent-input>

```

## Creating custom installation repositories with IBM Packaging Utility

**8.5.5.0**

IBM WebSphere Application Server Liberty uses IBM Installation Manager for installation and lifecycle management. Installation Manager accesses source repositories that contain the content for a software product installation. Repositories are available on product media, in IBM-hosted web-based repositories, and from Passport Advantage. IBM Packaging Utility can help you create and customize enterprise repositories that contain the correct combination of products and maintenance levels needed for all aspects of your business.

### About this task

You use Installation Manager to connect to an Installation Manager repository (or set of repositories) to find products and service updates that are available to you for installation. An Installation Manager repository is simply a tree-structured file folder that includes product payload and metadata. You can install the software products that you need directly from an IBM web-based service repository or download and unpack compressed files from Passport Advantage and install the products from the resulting unpacked file folders. The result of unpacking the files is also considered to be an Installation Manager repository. Like any Installation Manager repository, these unpacked files can be hosted on an internal HTTP server, FTP server, or network mount in order to make them available to the organization.

Packaging Utility is a companion tool for Installation Manager with which you can create and manage custom Installation Manager repositories for your organization. You can copy multiple packages, maintenance levels, and fixes into a single repository. Packaging Utility copies from source repositories to your target custom repositories. Source repositories can include any accessible Installation Manager repository, including IBM web-hosted product repositories and unzipped Passport Advantage downloads.

For more information on Packaging Utility, go to the IBM Packaging Utility Information Center.

### Procedure

Use Packaging Utility to create custom or "enterprise" Installation Manager repositories that contain specific products and maintenance levels that fit the needs of your business.

As an administrator, you can control the content of your enterprise repository, which then can serve as the central repository to which your organization connects in order to perform product installations and updates.

Packaging Utility essentially copies from a set of source Installation Manager repositories to a target repository and eliminates duplicate artifacts, helping to keep the repository size as small as possible. You can also delete (or "prune") a repository, removing maintenance levels or products that are not needed. You can download the latest version of Packaging Utility from the IBM Support Portal.

Like Installation Manager, Packaging Utility has GUI and command-line interfaces. You must specify repository URLs for Installation Manager repositories that contain the offerings that you wish to copy. Installation Manager repository URLs follow this pattern:

`http://www.ibm.com/software/repositorymanager/offering_name`

**Note:** This location does not contain a web page that you can access using a web browser. For example, WebSphere Application Server Liberty product repositories are located at the following URLs:

- WebSphere Application Server Liberty Network Deployment Version 8.5  
`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85`
- WebSphere Application Server Liberty Network Deployment Trial Version 8.5  
`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.NDTRIAL.v85`

See Online product repositories for WebSphere Application Server offerings for additional product repositories.

The target repository that you create with Packaging Utility will always support a full installation; therefore, you cannot use Packaging Utility to create a repository that is only a copy of a fix pack. You can, however, create a repository that contains the minimum content to support direct installation to a fix-pack level. Consider the following two examples that use the Packaging Utility command-line interface (**PUCL.exe**) that is available in the Packaging Utility installation folder.

- **Example 1**

**Note:** Note that you must read the license agreement that you can find with the product files and then signify your acceptance of the license agreement by specifying **-acceptLicense** in the command as shown in the following example.

```
PUCL copy com.ibm.websphere.liberty.ND.v85
-repositories
  http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85
-target D:\LIB_ND_version
-prompt
-showProgress
-acceptLicense
```

Since no version number is specified with the offering name, this command will create a new repository that supports direct installation to the latest fix-pack level for WebSphere Application Server Liberty Version 8.5. This new repository does not support the installation of Version 8.5.5.0, but it does support the update from an existing Version 8.5.5.0 installation to the latest version.

- **Example 2**

```
PUCL copy com.ibm.websphere.liberty.ND.v85_8.5.5.0.20110503_0200
-repositories
  http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85
-target D:\LIB_ND
-prompt
-showProgress
-acceptLicense
```

```
PUCL copy com.ibm.websphere.liberty.ND.v85_8.5.5.1.20110829_1838
-repositories
  http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85
-target D:\LIB_ND
-prompt
-showProgress
-acceptLicense
```

The first command creates a target repository with WebSphere Application Server Liberty Version 8.5.5.0. The second command adds the Version 8.5.5.1 fix pack to the same repository. You can now use this resulting repository to install Version 8.5.5.0, install Version 8.5.5.1, or update from Version 8.5.5.0 to Version 8.5.5.1.

**Tip:** With some offerings, such as WebSphere SDK Java Technology Edition Version 7.0 for Liberty, you can use Packaging Utility with the **-platform** option (sometimes called "platform slicing") to create a repository that is scoped to the platforms and architectures that are used by your organization. This feature is available in command-line mode by specifying the **-platform** option with the `os` and `arch` arguments as shown in the following example:

```
PUCL copy com.ibm.websphere.liberty.IBMJAVA.v70
-repositories http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v70
-platform os=linux,arch=ppc64
-target D:\LIB_ND
-prompt
-showProgress
-acceptLicense</p>
```

Your repository can be scoped for platforms other than the one on which it is created or stored. For example, you can run Packaging Utility on a Windows system to create a repository with the content needed to install on a Linux system. During installation on Linux, you point Installation Manager to your custom repository.

The following table lists valid combinations for creating a local WebSphere SDK Java Technology Edition Version 7.0 for Liberty offering repository that is sliced by operating system and architecture.

*Table 91. Valid combinations for creating a local WebSphere SDK Java Technology Edition Version 7.0 for Liberty offering repository using the Packaging Utility*

Platform	Options	Resulting Repository
Windows	os=win32,arch=x86	32-bit repository for 32-bit Windows OS and 64-bit Windows
	os=win32.arch=x86_64	64-bit repository for 64-bit Windows
Linux Intel	os=linux,arch=x86	32-bit repository for 32-bit Linux Intel and 64-bit Linux Intel
	os=linux.arch=x86_64	64-bit repository for 64-bit Linux Intel
Linux Power®	os=linux,arch=ppc	32-bit repository for 32-bit Linux Power and 64-bit Linux Power
	os=linux.arch=ppc64	64-bit repository for 64-bit Linux Power
zLinux	os=linux,arch=s390	32-bit repository for 32-bit zLinux and 64-bit zLinux
	os=linux.arch=s390x	64-bit repository for 64-bit zLinux
AIX®	os=aix,arch=ppc	32-bit repository for 32-bit AIX and 64-bit AIX
	os=aix.arch=ppc64	64-bit repository for 64-bit AIX
Solaris Sparc	os=solaris,arch=sparc	32-bit repository for 32-bit Solaris Sparc and 64-bit Solaris Sparc
	os=solaris,arch=sparc64	64-bit repository for 64-bit Solaris Sparc
Solaris Intel	os=solaris,arch=x86_64	64-bit repository for 64-bit Solaris Intel
HP-UX Itanium	os=hpux,arch=ia64	64-bit repository for 64-bit HP-UX Itanium
z/OS	os=zos,arch=s390x	64-bit repository for z/OS

The following table lists valid combinations for creating a local WebSphere SDK Java Technology Edition Version 6.0 for Liberty offering repository that is sliced by operating system and architecture.

Table 92. Valid combinations for creating a local WebSphere SDK Java Technology Edition Version 6.0 for Liberty offering repository using the Packaging Utility

Platform	Options	Resulting Repository
Windows	os=win32,arch=x86	32-bit repository for 32-bit Windows OS and 64-bit Windows
	os=win32.arch=x86_64	64-bit repository for 64-bit Windows
Linux Intel	os=linux,arch=x86	32-bit repository for 32-bit Linux Intel and 64-bit Linux Intel
	os=linux.arch=x86_64	64-bit repository for 64-bit Linux Intel
Linux Power	os=linux,arch=ppc	32-bit repository for 32-bit Linux Power and 64-bit Linux Power
	os=linux.arch=ppc64	64-bit repository for 64-bit Linux Power
zLinux	os=linux,arch=s390	32-bit repository for 32-bit zLinux and 64-bit zLinux
	os=linux.arch=s390x	64-bit repository for 64-bit zLinux
AIX	os=aix,arch=ppc	32-bit repository for 32-bit AIX and 64-bit AIX
	os=aix.arch=ppc64	64-bit repository for 64-bit AIX
Solaris Sparc	os=solaris,arch=sparc	32-bit repository for 32-bit Solaris Sparc and 64-bit Solaris Sparc
	os=solaris,arch=sparc64	64-bit repository for 64-bit Solaris Sparc
Solaris Intel	os=solaris,arch=x86_64	64-bit repository for 64-bit Solaris Intel
HP-UX Itanium	os=hpx,arch=ia64	64-bit repository for 64-bit HP-UX Itanium

For more information on platform slicing, go to the IBM Packaging Utility Information Center.

## Using the launchpad to start Liberty installations

**8.5.5.0**

The launchpad console is the starting point for installing IBM WebSphere Application Server Liberty Network Deployment.

### Before you begin

- The launchpad is a web application. Before using the launchpad, you must have a supported web browser. The launchpad supports the following browsers:
  - **AIX** **HP-UX** **Linux** **Solaris** Mozilla Firefox Version 3.5 or later
  - **Windows** Internet Explorer Version 6.0 Service Pack 2 or later
- Install a supported web browser if one is not installed.
  - **AIX** **HP-UX** **Linux** **Solaris** Install a browser such as Mozilla Firefox. Download Firefox from the following location: <http://www.mozilla.org/products/firefox/>.
  - **Windows** Install a browser for the Windows operating system.
    - Download Internet Explorer from the following location: <http://www.microsoft.com/windows/ie/default.msp>

- Download Mozilla Firefox from the following location: <http://www.mozilla.org/products/firefox/>.

- **AIX** **HP-UX** **Linux** **Solaris** You must install the Bash shell package to use the launchpad application. Although the Bash shell must be installed, the Bash shell does not need to be used to run the **launchpad.sh** command. If you attempt to run the launchpad application from a DVD on the HP-UX, Linux, or Solaris operating systems without the Bash shell installed, the launchpad fails with an error message indicating that the Bash interpreter is not found. If you attempt to run the launchpad from any image on AIX, the launchpad fails with an error message indicating that the current browser is not supported. The Bash package for the AIX operating system is included in the IBM AIX Toolbox.

#### Examples of what the launchpad can do:

- The launchpad does support installing Installation Manager in admin or non-admin (user) mode.
- The launchpad does support updating Installation Manager from an earlier version in admin or non-admin (user) mode.

#### Examples of what the launchpad cannot do:

- The launchpad does not support installing in group mode.
- The launchpad does not support installing or updating with a custom application data location.

**Restriction:** You cannot run the launchpad remotely to install a product. Only local use of the launchpad is supported.

#### About this task

The launchpad identifies components on the product disk or image that you can install (launch).

The launchpad is a single point of reference for installing the application server environment. If you click a link that points to a product repository on another disk or image, you are prompted to insert that disk or browse to that image.

#### Procedure

1. Start the launchpad.

The launchpad program is available in the root directory of the product disk. You can start the launchpad manually using a fully qualified command instead of changing directories to the disk and running the command locally from the root directory:

- **AIX** **HP-UX** **Linux** **Solaris** Mount the disk drive if necessary.
- Open a shell window and issue a fully qualified **launchpad** command to start the launchpad.

**Tip:** **Windows** If you need to navigate using the keyboard, use Mozilla Firefox as your web browser and start the launchpad with the following command:

```
launchpad_all.y.exe
```

**Note:** **Windows** Some Windows operating systems such as Windows 2003, Windows Vista, Windows Server 2008, and Windows 7 have implemented a more restrictive security policy that denies access to trusted files by non-trusted files or applications. When the launchpad application is run as a non-trusted program, you will receive JavaScript "Access is denied" errors that subsequently cause the application to hang. Because downloaded images are automatically blocked, unblock the files so that the launchpad can successfully access the files. Before you extract the image, right-click the image file and select **Properties** to open the Properties panel and locate the security section and click the **Unblock** button. You can now extract the image and run the launchpad application. The launchpad opens in the language of the locale setting of the machine.

2. Use the launchpad to perform the following Liberty related tasks.

- View the Welcome page, and access links to the IBM WebSphere Application Server Information Center and the IBM Education Assistant.
- Launch IBM Installation Manager installation, and access the IBM Installation Manager Information Center.
- Launch IBM Packaging Utility installation, and access the Packaging Utility information in the IBM Installation Manager Information Center.
- Launch Installation Manager to install WebSphere Application Server Liberty Network Deployment, and access the installation instructions in the information center.
- Launch Installation Manager to install IBM HTTP Server, and access the installation instructions in the information center.
- Launch Installation Manager to install Web Server Plug-ins for IBM WebSphere Application Server, and access the installation instructions in the information center.
- Access the latest version of IBM Support Assistant.
- Launch Installation Manager to install IBM WebSphere SDK Java Technology Edition Version 6.0 for Liberty, and access the installation instructions in the information center.
- Launch Installation Manager to install IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty, and access the installation instructions in the information center.
- Launch Installation Manager to install the IBM WebSphere Application Server Web 2.0 and Mobile Toolkit, and access the installation instructions in the information center.
- Launch Installation Manager to install IBM WebSphere Adapters.

## Results

This procedure results in using the launchpad to start the installation and to access information through a browser.

### Troubleshooting

If you can start the launchpad but clicking a link does not resolve to a page in the launchpad, you might have the wrong media in the disk drive. Check the validity of the media.

Use the following procedure to correct any error that is preventing the launchpad from displaying. Then, try to start the launchpad again:

1. If the product disk is no longer accessible, insert the disk.
2. **AIX** **HP-UX** **Linux** **Solaris** Mount the drive as necessary on platforms such as AIX or Linux.
3. Enable the JavaScript function in your browser.
 

Mozilla Firefox: Click **Tools** > **Options** > **Content**:

  - Select **Enable Java**.
  - Select **Enable JavaScript**.
  - Click **Advanced** and allow scripts to ... (Select all boxes.)

**Windows** Internet Explorer: Click **Tools** > **Internet Options** > **Security** > **Custom Level for Internet > Scripting** > **Active scripting** > **Enable**.
4. Restart the launchpad by issuing the **launchpad** command.

If the launchpad links still do not work after following this procedure, launch Installation Manager and point it at the appropriate repositories to install the offerings.

## What to do next

Go to “Installing and uninstalling Liberty on distributed operating systems” on page 1165 to continue installing your application serving environment.

## Installing and uninstalling Liberty on IBM i operating systems

8.5.5.0

IBM Installation Manager is a common installer for many IBM software products. You can use Installation Manager to install and manage the product lifecycle of WebSphere Application Server Liberty Network Deployment.

### Before you begin

**Note:** 8.5.5.11 Support for using Java SE 6 with WebSphere Liberty ends in September 2017. After the end of support, the Liberty kernel will be recompiled and can no longer run with Java SE 6. If you continue to use Java SE 6 on earlier fix packs after the end of support date, you could expose your environment to security risks.

Java SE 8 is the recommended Java SDK because it provides the latest features and security updates.

Installation Manager is a single installation program that can use remote or local software repositories to install, modify, or update WebSphere Application Server Liberty Network Deployment. It determines available packages - including products, fix packs, interim fixes, and so on - checks prerequisites and interdependencies, and installs the selected packages. You also use Installation Manager to uninstall the packages that it installed.

**Restriction:** The Installation Manager GUI is not available on IBM i; all interaction with Installation Manager on IBM i is done through the command line or response files.

**Overview of IBM Installation Manager:** IBM Installation Manager is a general-purpose software installation and update tool that runs on a range of computer systems. Installation Manager can be invoked through a command-line interface. You can also create response files in XML and use them to direct the performance of Installation Manager tasks in silent mode.

For more information on using Installation Manager, read the IBM Installation Manager Information Center.

**Packages and package groups:** Each software product that can be installed with Installation Manager is referred to as a package. An installed package has a product level and an installation location. A package group consists of all of the products that are installed at a single location.

**How many Installation Managers do you need:** You only need to run Installation Manager on those systems on which you install or update product code. You normally need only one Installation Manager on a system because one Installation Manager can keep track of any number of product installations.

**Creating an Installation Manager:** When the installation kit is available on your system, you can create an Installation Manager. An Installation Manager consists of a set of binaries that are copied from the installation kit and a set of runtime data that describe the products that have been installed by this particular Installation Manager. Before creating an Installation Manager, you must decide in which mode the Installation Manager will run as well as where the binaries and runtime data - called agent data or appdata - will reside. Then, you issue the Installation Manager installation command from the appropriate user ID to create the Installation Manager.

**Accessing product repositories:** All software materials that will be installed with IBM Installation Manager are stored in repositories. Each repository contains program objects and metadata for one or more packages - that is, software products at a particular level. Repositories can also contain product maintenance, such as fix packs and interim fixes. Whenever you install a new product, you can choose from any of the available product levels in any accessible repository.

**Installing the product:** After you have created an Installation Manager and have access to all necessary product repositories, you can use Installation Manager command-line commands or response files to perform the actual product installations. When you install a product, you provide the package name, optionally the product level to be installed, the product location, and any other optional properties. For example, some products have optional features that you can select at installation time or a list of optional supported language packs from which you can select.

**Working with installed products:** You can use Installation Manager commands to list installed products and product levels. You can also obtain this information for installed copies of WebSphere Application Server Liberty Network Deployment by issuing the **versionInfo** command from the product file system. You can use Installation Manager commands or response files to install a new product level, roll back to a previous level, or modify the product by adding or removing optional features or language packs.

#### Notes:

- You must have Java SE 6 32 bit (option 11 of the IBM Developer Kit for Java) installed on your IBM i system before installing WebSphere Application Server Liberty Network Deployment. For more information, read IBM i prerequisites.
- Do not transfer the content of a repository in non-binary mode and do not convert any content on extraction.
- When you try to install IBM Installation Manager locally from the WebSphere Application Server Liberty Network Deployment media on an IBM i operating system, the following error message might be displayed:

The Installc executable launcher was unable to locate its companion shared library.

This error occurs because all directory and files names contained by the media are displayed in uppercase. To resolve this issue, enable the handling of mixed case on your IBM i operating system using the following command:

```
CHGOPTA EXTMEDFMT(*YES)
```

- **8.5.5.1** If you are installing WebSphere Application Server Liberty Version 8.5.5.1 in console mode, you might receive warning messages similar to the following example:

```
No "conClass" attribute in "commonPanel" element of panel com.ibm.was.liberty.userdata.panel.UserData in com.ibm.was.liberty.userdata.panel.
```

This problem is caused by an IBM Installation Manager API which is deprecated in Version 1.6.2. These warning messages can be ignored. No action is required.

## About this task

For more information on using Installation Manager, read the IBM Installation Manager Information Center.

Perform one of these procedures to install, update, rollback, or uninstall the offering using Installation Manager.

**Note:** Before using Installation Manager to install a offering, you might want to back up your Installation Manager configuration using the instructions in the IBM Installation Manager Information Center if the possibility of corruption is a concern.

## Procedure

- “Installing Liberty on IBM i operating systems using response files” on page 1299
- “Installing Liberty on IBM i operating systems using the command line”
- “Installing Liberty remotely on IBM i operating systems using the **iRemoteInstall** command” on page 1304
- “Adding and removing features from Liberty on IBM i operating systems using response files” on page 1312
- “Installing Liberty interim fixes on IBM i operating systems using the command line” on page 1315
- “Uninstalling Liberty interim fixes from IBM i operating systems using the command line” on page 1326
- “Installing Liberty fix packs on IBM i operating systems using response files” on page 1323
- “Installing Liberty fix packs on IBM i operating systems using the command line” on page 1318
- “Uninstalling Liberty fix packs from IBM i operating systems by using response files” on page 1329
- “Uninstalling Liberty fix packs from IBM i operating systems using the command line” on page 1327
- “Uninstalling Liberty from IBM i operating systems using response files” on page 1315
- “Uninstalling Liberty from IBM i operating systems using the command line” on page 1314

## Results

- The following locations are the defaults for Installation Manager files on IBM i systems:
  - **Installation location:** /QIBM/ProdData/InstallationManager
  - **Agent data location:** /QIBM/UserData/InstallationManager
  - **Registry:** /QIBM/InstallationManager/.ibm/registry/InstallationManager.dat
- Logs are located in the logs directory of Installation Manager's agent data location. For example:

/QIBM/UserData/InstallationManager/logs

The main log files are time-stamped XML files in the logs directory, and they can be viewed using any standard web browser.

## Installing Liberty on IBM i operating systems using the command line

**8.5.5.0**

You can install WebSphere Application Server Liberty Network Deployment on IBM i operating systems using the Installation Manager command line.

### Before you begin

Prepare for the installation before using this procedure. See [Preparing the operating system for installation on IBM i](#) for more information.



**8.5.5.6**

If you want to install Liberty assets from local directory-based repositories or an instance of the Liberty Asset Repository Service, configure the repositories. For more information about the Liberty asset repositories, see [“Installing assets using Installation Manager”](#) on page 1411.

**Important:** Before installing WebSphere Application Server Liberty Network Deployment, you must read the license agreement that you can find with the product files. Signify your acceptance of the license agreement by specifying **-acceptLicense** in the command as described in this topic.

**Install Installation Manager** on the system onto which you want to install the product.

- If you want to use the Installation Manager that comes with this product, perform the following actions:

1. Obtain the necessary files.

There are three basic options for obtaining and installing Installation Manager and the product.

– **Access the physical media, and use local installation**

You can access the product repositories on the media.

a. Install Installation Manager on your system.

You can install Installation Manager using the media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

b. Use Installation Manager to install the product from the product repositories on the media.

– **Download the files from the Passport Advantage site, and use local installation**

Licensed customers with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

a. Download the files from the Passport Advantage site.

b. Install Installation Manager on your system.

You can install Installation Manager using the media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

c. Use Installation Manager to install the product from the downloaded repositories.

– **Access the live repositories, and use web-based installation**

If you have a Passport Advantage ID and password, you can install the product from the web-based repositories.

a. Install Installation Manager on your system.

You can install Installation Manager using the media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

b. Use Installation Manager to install the product from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85>

**Note:** This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify for the value of the `-repositories` parameter so that the `imcl` command can access the files in this repository to install the product.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

**Note:** If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

2. Choose three separate locations for Installation Manager's binaries, runtime data (agent data), and shared data locations.

3. Install Installation Manager using the Installation Manager command line.

a. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.

b. On a CL command line, run the **STRQSH** command to start the Qshell command shell.

c. Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

To set the umask setting to 022, issue the following command:

```
umask 022
```

- d. Change to the location containing the Installation Manager installation files, and run the following command:

```
installc -acceptLicense -log log_file_path_and_name
```

**Notes:**

- For more information on installing Installation Manager, see the IBM Installation Manager Information Center.
- Use only the **installc** command to install Installation Manager.
- If you already have a version of Installation Manager installed on your system and you want to use it to install and maintain the product, obtain the necessary product files.

There are three basic options for installing the product.

- **Access the physical media, and use local installation**

You can access the product repositories on the media. Use Installation Manager to install the product from the product repositories on the media.

- **Download the files from the Passport Advantage site, and use local installation**

Licensed customers with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

1. Download the product repositories from the Passport Advantage site.
2. Use Installation Manager to install the product from the downloaded repositories.

- **Access the live repositories, and use web-based installation**

If you have a Passport Advantage ID and password, you can use Installation Manager to install the product from the web-based repositories. Use Installation Manager to install the product from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85>

**Note:** This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify for the value of the **-repositories** parameter so that the **imcl** command can access the files in this repository to install the product.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

**Note:** If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

## About this task

**8.5.5.4** To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

## Procedure

1. Optional: If the repository requires a username and password, create a credential-storage file to access this repository.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the **imutilsc** command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store

credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

2. Choose three separate locations for the product's binaries, runtime data (agent data), and shared data locations.
3. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
4. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
5. Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

To set the umask setting to 022, issue the following command:

```
umask 022
```

6. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
7. Use the **imcl** command to install the product.

```
./imcl install com.ibm.websphere.liberty.ND.v85_offering_version,optional_feature_ID  
-repositories source_repository  
-installationDirectory installation_directory  
-sharedResourcesDirectory shared_directory  
-preferences preference_key=value  
-properties property_key=value  
-secureStorageFile storage_file -masterPasswordFile master_password_file  
-acceptLicense
```

### Tips:

- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lafiles` or `product_name/lafiles` subdirectory of the installation image or repository for this offering.
- You can install a list of features that are separated by commas.
  - Embeddable EJB container and JPA client (`embeddablecontainer`)

This option installs the embeddable EJB container and JPA client.

The embeddable EJB container is a Java Archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition (SE) environment. You can run enterprise beans using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.

The JPA client can be used with the embeddable EJB container to provide Java Persistence API capability in a Java SE environment.

- Extended Programming Models - `extprogmodels` (for fix pack 8.5.5.3 and earlier versions)

The Extended Programming Models feature provides a rich set of programming models such as Web Services, JMS (including Message-Driven Beans), and Mongo 2.0.

### Notes:

- If no features are specified, the default features (`embeddablecontainer` and `extprogmodels`) are installed. To install only the feature that you want, specify that feature explicitly.

-  **8.5.5.2** You can specify additional assets to install from the Liberty Repository. For a list of Liberty Repository assets, see the downloads page on WASdev.net.

To install assets from the IBM WebSphere Liberty Repository, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later.

If you want to install Liberty Repository features, specify the short names or symbolic names on the **user.feature** option of the **-properties** parameter. Multiple feature names are separated with double commas. The following example installs the Portlet Container and Portlet Serving features:

```
-properties user.feature=portlet-2.0,,portletserving-2.0,user.accept.license=true
```

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.



**8.5.5.4**

Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` addon, or install the individual features that you need from the Liberty Repository. See the following topics for more information:

- Installing Liberty Repository assets
- Liberty features

You can install the complete set of Extended Programming Model features by specifying the `user.addon` option:

```
-properties user.addon=extendedPackage-1.0,user.accept.license=true
```

If you upgrade WebSphere Application Server Liberty Version 8.5.5.3 or previous versions that contain the `extprogmodels` feature, Installation Manager automatically installs the `extendedPackage-1.0` add-on. You must specify the `user.accept.license` option:

```
-properties user.accept.license=true
```



**8.5.5.6**

You can also install assets from instances of the Liberty Asset Repository Service or local directory-based repositories. For more information about these asset repositories, see “Installing assets using Installation Manager” on page 1411. Add the repository on the `-repositories` parameter. The repositories are accessed in the order that they are specified. By default, the Liberty Repository is the last of the repositories that are accessed during installation. To disable access to the Liberty Repository, on the `-properties` parameter, set the `user.useLibertyRepository` option to `false`.

**8.5.5.8**

```
./imcl install com.ibm.websphere.liberty.nd.v85
-properties user.useLibertyRepository=false,user.addon=extendedPackage-1.0,user.feature=portlet-2.0
-installationDirectory /QIBM/ProdData/Liberty -acceptLicense
-repositories /QIBM/LibertyProductRepo,https://your_onprem_asset_repo_url,/QIBM/LocalAssetRepo,/QIBM/LocalAssetRepo2.zip
-sharedResourcesDirectory /QIBM/UserData/InstallationManager/IMShared
-showProgress
```

To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.

- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.5.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
./imcl listAvailablePackages -repositories source_repository
```

- You can also specify `none`, `recommended` or `all` with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the `-installFixes` option defaults to `all`.
  - If the offering version is specified, the `-installFixes` option defaults to `none`.
- For initial installations, it is a good practice to specify the *user\_data\_root*; otherwise, the default value for the *user\_data\_root*, `/QIBM/UserData/WebSphere/AppServer/V85/ND`, is used. Use the `was.install.os400.profile.location` property to specify the *user\_data\_root*. If the *user\_data\_root* is to be `/QIBM/UserData/WebSphere/AppServer/V85/ND_1`, for example, specify `-properties was.install.os400.profile.location=/QIBM/UserData/WebSphere/AppServer/V85/ND_1` on the `imcl` installation command.
- The program might write important post-installation instructions to standard output.

For more information on using the `imcl` command to install the product, see the IBM Installation Manager Information Center.

## Example

The following example uses the **imcl** command to install WebSphere Application Server Liberty Network Deployment:

```
./imcl install com.ibm.websphere.liberty.ND.v85
-repositories https://downloads.mycorp.com:8080/WAS_85_repository
-installationDirectory /QIBM/ProdData/WebSphere/AppServer/V85/ND
-properties was.install.os400.profile.location=/QIBM/UserData/WebSphere/AppServer/V85/ND
-sharedResourcesDirectory /QIBM/UserData/InstallationManager/IMShared
-secureStorageFile $HOME/WASFiles/temp/credential.store -masterPasswordFile $HOME/WASFiles/IM/master_password_file.txt
-acceptLicense
```

## Installing Liberty on IBM i operating systems using response files

**8.5.5.0**

You can install WebSphere Application Server Liberty on IBM i operating systems using Installation Manager response files.

### Before you begin

Prepare for the installation before using this procedure. See *Preparing the operating system for installation on IBM i* for more information.



**8.5.5.6**

If you want to install Liberty assets from local directory-based repositories or an instance of the Liberty Asset Repository Service, configure the repositories. For more information about the Liberty asset repositories, see “Installing assets using Installation Manager” on page 1411.

Before you install WebSphere Application Server, ensure that your user profile has \*ALLOBJ and \*SECADM special authorities.

**Install Installation Manager** on the system onto which you want to install the product.

**8.5.5.4**

To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

- If you want to use the Installation Manager that comes with this product, perform the following actions:

1. Obtain the necessary files.

There are three basic options for obtaining and installing Installation Manager and the product.

– **Access the physical media, and use local installation**

You can access the product repositories on the media.

- a. Install Installation Manager on your system.

You can install Installation Manager using the media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- b. Use Installation Manager to install the product from the product repositories on the media.

– **Download the files from the Passport Advantage site, and use local installation**

Licensed customers with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

- a. Download the files from the Passport Advantage site.

- b. Install Installation Manager on your system.

You can install Installation Manager using the media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

- c. Use Installation Manager to install the product from the downloaded repositories.

– **Access the live repositories, and use web-based installation**

If you have a Passport Advantage ID and password, you can install the product from the web-based repositories.

a. Install Installation Manager on your system.

You can install Installation Manager using the media, using a file obtained from the Passport Advantage site, or using a file containing the most current version of Installation Manager from the IBM Installation Manager download website.

b. Use Installation Manager to install the product from the web-based repository located at

`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85`

**Note:** This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify in the response file so that the installation can access the files in this repository.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

**Note:** If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

2. Install Installation Manager.

a. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.

b. On a CL command line, run the **STRQSH** command to start the Qshell command shell.

c. Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

To set the umask setting to 022, issue the following command:

```
umask 022
```

d. Change to the temporary directory where you unpacked the Installation Manager files.

e. Run the following command in the temporary folder:

```
installc -acceptLicense -log log_file_path_and_name
```

**Notes:**

– For more information on installing Installation Manager, see the IBM Installation Manager Information Center.

– Use only the **installc** command to install Installation Manager.

- If you already have a version of Installation Manager installed on your system and you want to use it to install and maintain the product, obtain the necessary product files.

There are three basic options for installing the product.

– **Access the physical media, and use local installation**

You can access the product repositories on the media. Use Installation Manager to install the product from the product repositories on the media.

– **Download the files from the Passport Advantage site, and use local installation**

Licensed customers with a Passport Advantage ID and password can download the necessary product repositories from the Passport Advantage site.

1. Download the product repositories from the Passport Advantage site.

2. Use Installation Manager to install the product from the downloaded repositories.

– **Access the live repositories, and use web-based installation**

If you have a Passport Advantage ID and password, you can use Installation Manager to install the product from the web-based repositories. Use Installation Manager to install the product from the web-based repository located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85>

**Note:** This location does not contain a web page that you can access using a web browser. This is a remote web-based repository location that you must specify in the response file so that the installation can access the files in this repository.

Whenever possible, you should use the remote web-based repositories so that you are accessing the most up-to-date installation files.

**Note:** If you do not have a Passport Advantage ID and password, you must install the product from the product repositories on the media or local repositories.

## Procedure

1. Optional: If the repository requires a username and password, create a credential-storage file to access this repository.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutils` command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the `-keyring` and `-password` options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the `-keyring` and `-password` options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

2. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
3. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
4. Make sure that the `umask` is set to 022.

To verify the `umask` setting, issue the following command:

```
umask
```

To set the `umask` setting to 022, issue the following command:

```
umask 022
```

5. Use a response file to install the product.

Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and install the product. For example:

```
./imcl -acceptLicense  
input $HOME/WASFiles/temp/install_response_file.xml  
-log $HOME/WASFiles/temp/install_log.xml  
-secureStorageFile $HOME/WASFiles/temp/credential.store -masterPasswordFile $HOME/WASFiles/master_password_file.txt
```

### Notes:

- The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lafiles` or `product_name/lafiles` subdirectory of the installation image or repository for this offering.
- `/QIBM/ProdData/InstallationManager` is the default installation location for Installation Manager files on IBM i systems.
- The program might write important post-installation instructions to standard output.

Read the IBM Installation Manager Information Center for more information.

## Example

The following is an example of a response file for installing the product with no optional features into the /QIBM/ProdData/WebSphere/AppServer/V85/ND directory using a web-based repository located at <http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85>.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85' />
</server>
<profile id='WebSphere Liberty V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/ND' />
  <data key='user.import.profile' value='false' />
</profile>
<install modify='false'>
  <offering profile='WebSphere Liberty V8.5'
    features='' id='com.ibm.websphere.liberty.ND.v85' />
</install>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache'
  value='/QIBM/UserData/InstallationManager/IMShared' />
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
<preference name='offering.service.repositories.areUsed' value='true' />
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
<preference name='http.ntlm.auth.kind' value='NTLM' />
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
<preference name='PassportAdvantageIsEnabled' value='false' />
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
</agent-input>
```

### Tips:

- Make sure that the repository location points to the web-based or local product repository. For example:

```
<repository location='https://downloads.mycorp.com:8080/WAS_85_repository' />
```

- The following line from the example specifies the default value of the profile location for IBM i:

```
<data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/ND' />
```

To override this default location, specify a different location

- The following line from the example specifies the default value of the shared resources directory for IBM i:

```
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared' />
```

To override this default location, specify a different location

**Note:** There is only one shared resources directory for Installation Manager. If there has been an installation on the system in the past, it will use that shared resources directory and not the one specified in the response file.

- To disable remote searches for updates in the response file, set the following preferences to false:

- offering.service.repositories.areUsed

Used for searching remote repositories for updates to installed offerings

- com.ibm.cic.common.core.preferences.searchForUpdates

Used for searching for updates to Installation Manager

For example:

```
<preference value='false' name='offering.service.repositories.areUsed' />
<preference value='false' name='com.ibm.cic.common.core.preferences.searchForUpdates' />
```

You can find more details on silent preference keys in the IBM Installation Manager Information Center.

- To install more than one instance of an offering, you must make the profile ID of each additional instance unique. For example:

```
<offering profile='WebSphere Liberty V8.5 - Another User's WAS Liberty ND'  
  features='' id='com.ibm.websphere.liberty.ND.v85' />
```

This must be changed in both places that specify the profile ID in the response file.

Here are some examples of changes that you could make to manipulate this response file to perform alternative actions.

- To alter the location of the installation, simply change the installation location. For example:

Replace

```
<profile id='WebSphere Liberty V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
```

with

```
<profile id='WebSphere Liberty V8.5' installLocation='/home/user/IBM/WebSphere/AppServer/V85/Server'>
```

- To install from a local repository instead of the live remote repository, replace the repository location. For example:

Replace

```
<repository location='http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85' />
```

with

```
<repository location='/home/user/repositories/WAS85/local-repositories' />
```

- To add the optional features, add each desired feature in the offering as an entry in a comma-separated list.

In the following list, the offering IDs to be used in the response files are enclosed in parentheses:

- Embeddable EJB container and JPA client (embeddablecontainer)

This option installs the embeddable EJB container and JPA client.

The embeddable EJB container is a Java Archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition (SE) environment. You can run enterprise beans using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.

The JPA client can be used with the embeddable EJB container to provide Java Persistence API capability in a Java SE environment.

- Extended Programming Models (extprogmodels) - Versions 8.5.5.0 to 8.5.5.3

The Extended Programming Models feature provides a rich set of programming models such as Web Services, JMS (including Message-Driven Beans), and MongoDB 2.0.

#### Notes:

- If no features are specified, the default features (embeddablecontainer and extprogmodels) are installed. To install only the feature that you want, specify that feature explicitly.

For example, to install the Embeddable EJB container:

Replace

```
<offering profile='WebSphere Liberty V8.5'  
  features='' id='com.ibm.websphere.liberty.ND.v85' />
```

with

```
<offering profile='WebSphere Liberty V8.5'  
  features='embeddablecontainer' id='com.ibm.websphere.liberty.ND.v85' />
```

-  **8.5.5.2** You can specify additional assets to install from the Liberty Repository. For a list of Liberty Repository assets, see the downloads page on WASdev.net.

To install Liberty Repository assets, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later. Previous versions of Installation Manager do not have the

option to install Liberty Repository assets. If you use a response file and did not update Installation Manager to Version 1.6.2 or later, the assets that you specify in the response file are ignored during installation.

If you want to install additional features, specify two extra data key elements in your response file. You can use either the symbolic name or the short name.

The following example installs the Portlet Container and Portlet Serving features using the symbolic name.

```
<data key='user.feature' value='com.ibm.websphere.appserver.portlet-2.0,,com.ibm.websphere.appserver.portletserving-2.0' />
<data key='user.accept.license' value='true' />
```

The following example installs the Portlet Container and Portlet Serving features using the short name:

```
<data key='user.feature' value='portlet-2.0,,portletserving-2.0' />
<data key='user.accept.license' value='true' />
```

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.



**8.5.5.4**

Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` addon, or install the individual features that you need from the Liberty Repository. See the following topics for more information:

- Installing Liberty Repository assets
- Liberty features

The following example installs the Extended Programming Models using the `user.addon` parameter and the Portlet Container and Portlet Serving features using the `user.feature` parameter with short names:

```
<data key='user.addon' value='extendedPackage-1.0' />
<data key='user.feature' value='portlet-2.0,,portletserving-2.0' />
<data key='user.accept.license' value='true' />
```



**8.5.5.6**

You can also install assets from an instance of the Liberty Asset Repository Service or local directory-based repositories. For more information, see “Installing assets using Installation Manager” on page 1411. Add the repository on `repository` elements. If Installation Manager does not recognize the repository, point directly to the `repository.config` file. When you install assets, the repositories are accessed in the order that you specify them.

```
<server>
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85" />
<repository location="https://your_onprem_asset_repo_url" />
<repository location="/QIBM/LocalAssetRepo" />
```

**8.5.5.8**

`<repository location="/QIBM/LocalAssetRepo2.zip" />` By default, the Liberty Repository is the last of the repositories that are accessed during installation. To disable access to the Liberty Repository, set the `user.useLibertyRepository` parameter to `false`:

```
<data key='user.addon' value='extendedPackage-1.0' />
<data key='user.feature' value='portlet-2.0,,portletserving-2.0' />
<data key='user.useLibertyRepository' value='false' />
```

To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.

## Installing Liberty remotely on IBM i operating systems using the `iRemoteInstall` command

**8.5.5.0**

You can use the `iRemoteInstall` command to install IBM Installation Manager or WebSphere Application Server Liberty Network Deployment from a Windows workstation to a remote target IBM i system.

### Before you begin

Prepare for the installation before using this procedure. See Preparing the operating system for installation on IBM i for more information.

The product offering repository files or the IBM Installation Manager for IBM i installation kit compressed file must be available on the Windows system.

**Important:** You must set your JAVA\_HOME environment variable to your IBM Installation Manager JRE home before running the command directly from the media.

#### Restrictions:

- The **iRemoteInstall** command does not support credential-storage files used to pass confidential information. You must use the physical media or download the installation files to your local system.
- The **iRemoteInstall** command does not support the use of response files.

#### About this task

**Note:** By running this script, you accept the terms of the product license. The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lafiles` or `offering_name/lafiles` subdirectory of the installation image or repository for this offering.

#### Location of the iRemoteInstall command:

The **iRemoteInstall** command is located in the following directory when it has been installed as part of the WebSphere Customization Toolbox:

```
wct_root/Remote_Installation_Tool_for_IBM_i
```

**Tip:** A version of this utility that is current when the product is released is also available on the media or installation image. You can run the command directly from the media connected to a Windows system to install the offering on a remote target IBM i system. This version of the utility is located at the following location:

```
media_root\Remote_Installation_Tool_for_IBM_i\iRemoteInstall.bat
```

where *media\_root* is the root directory of the media or installation image containing the product or supplements.

#### Syntax of the iRemoteInstall command:

```
iRemoteInstall.bat
-hostname i5_hostname
-username user_login_name
-password user_login_password
-iminstit im_install_kit_file_path_and_name | -wasoid was_offering_id
-wasrepoloc was_install_file_location
-appdataloc im_agent_data_location
-wasinstloc was_install_location
-wassharedloc was_shared_location
-features feature_ID_1,feature_ID_2, . . .
-properties key=value,key=value, . . .
-log log_file_path_and_name
-trace
-version
-help
```

#### Parameters of the iRemoteInstall command:

##### **-hostname *i5\_hostname***

Specifies the host name of the target IBM i machine to which Installation Manager or WebSphere Application Server Liberty Network Deployment is going to be installed.

This parameter is required.

##### **-username *user\_login\_name***

Specifies the login name of the user who is performing the Installation Manager or WebSphere Application Server Liberty Network Deployment remote installation.

This user must be a valid user for the target IBM i system with \*ALLOBJ and \*SECADM special authorization.

##### **-password *user\_login\_password***

Specifies the login password of the user specified in **-username**.

- iminstkit *im\_install\_kit\_file\_name***  
 Specifies the location of the Installation Manager for IBM i installation kit  
 You must include the path if it is not in the same directory as the command.  
 This parameter is required.
- wasoid *was\_offering\_id***  
 Specifies the ID of the WebSphere Application Server Liberty offering being installed  
 Example values are base, nd, express, etc. This parameter is not case sensitive.  
 The value to use can be found in the product offering ID. If the offering ID is com.ibm.websphere.liberty.XXX.v85, for example, the **-wasoid** value should be liberty.XXX.
- wasrepoloc *was\_install\_file\_location***  
 Specifies the location of the WebSphere Application Server Liberty Network Deployment installation repository  
 This option must be specified if the **-wasoid** parameter is specified.
- appdataloc *im\_agent\_data\_location***  
 Specifies the location of the Installation Manager agent data  
 If no value is specified for this parameter, it is set to the default value of /QIBM/UserData/InstallationManager.
- wasinstloc *was\_install\_location***  
 Specifies the location of the WebSphere Application Server Liberty Network Deployment installation  
 If no value is specified for this parameter, it is set to the default value of /QIBM/WAS85/Liberty.
- wassharedloc *was\_shared\_location***  
 Specifies the location of the WebSphere Application Server Liberty Network Deployment shared location  
 If no value is specified for this parameter, it is set to the default value of /QIBM/WAS85/Liberty\_Shared.
- features *feature\_ID\_1,feature\_ID\_2, . . .***  
 Specifies the features to be installed  
 The feature IDs must be separated by commas (,).
- Tip:** If no features are specified, the default features (embeddablecontainer and extprogmodels) are installed. To install only the feature that you want, specify that feature explicitly.
- properties *key=value,key=value, . . .***  
 Specifies package-group (profile) properties
- log *log\_file\_path\_and\_name***  
 Turns on the log, and sends all messages to the specified file and location  
 The path can be absolute (c:\temp\mylog.log for example) or relative (..\mylog.log for example).  
 Because you can append multiple installation actions into the same log, the actual name of a log file that is generated is *log\_file\_path\_and\_name.x.log*, where *x* is the number of the log file from 0 to 29. The maximum log file size is approximately 10 MB; and the maximum number of log files generated is 30.
- trace**  
 Provides trace output of what the command checks and what the command discovers

**-version**

Displays the version information for the command

**-help**

Displays usage information for the command

**Procedure**

1. Log in to the IBM i machine using the IBM Personal Communications tool, or telnet with TN5250 to the IBM i machine.
2. If TCP/IP is not started or if you do not know if TCP/IP is started, enter the following command on the Control Language (CL) command line:

```
STRTCP
```

3. Verify that the host server jobs are started on your IBM i server.

The host server jobs allow the installation code to run on IBM i.

Enter the following command on the CL command line:

```
STRHOSTSVR SERVER(*ALL)
```

4. Verify that your user profile has \*ALLOBJ and \*SECADM special authorities.
5. Run the **iRemoteInstall** command in the temporary directory to install Installation Manager or Websphere Application Server Liberty Network Deployment.  
In order to install Websphere Application Server Liberty Network Deployment, Installation Manager must already be installed on the target system.
6. Verify the installation.
  - Check for error messages in the output from the **iRemoteInstall** command.
  - Look for errors in the installation log.

**Example**

Here is an example of installing IBM Installation Manager with the **iRemoteInstall** command:

```
./iRemoteInstall
-hostname iserver1.somedomain.com
-username wasadmin -password mypwd
-iminstit E:\agent.installer.os400.motif.ppc_1.6.2000.20101206_0100.zip
```

Here is an example of installing WebSphere Application Server Liberty Network Deployment with the **iRemoteInstall** command:

```
./iRemoteInstall
-hostname iserver1.somedomain.com
-username wasadmin -password mypwd
-wasoid liberty.ND
-wasrepoloc E:\repository
```

**Verifying the installation**

**8.5.5.0**

You can verify successful installation of the offering using the capabilities of IBM Installation Manager.

**Procedure**

- To verify installation of the offering, you can use Installation Manager to find the offering in the list of installed packages.

Change the directory to the `eclipse/tools` subdirectory of the Installation Manager binaries location, and run this command:

```
./imcl listInstalledPackages
```

This will display a list indicating which packages this Installation Manager has installed. For example:

```
com.ibm.websphere.liberty.ND.v85_8.5.5.20110203_0234
```

- If an installation was successful, the `installed.xml` file should contain a location element for the installed offering.

For example, the following file:

```
installation_manager_root/properties/version/installed.xml
```

should contain something like this:

```
<location id="IBM WebSphere Application Server Liberty Network Deployment V8.5" kind="product" path="/QIBM/ProdData/WebSphere/AppServer/V85/ND"> ..... </location>
```

- If you used the Installation Manager **-log** option during installation, you can verify that the resulting log file does not contain any errors.

If you used the following command to install the offering silently for example:

```
./imcl -acceptLicense
input $HOME/WASFiles/liberty/temp/install_response_file.xml
-log $HOME/WASFiles/liberty/temp/install_log.xml
-secureStorageFile $HOME/WASFiles/liberty/temp/credential.store -masterPasswordFile $HOME/WASFiles/liberty/master_password_file.txt
```

and the installation was successful, the `install_log.xml` file should contain something like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
</result>
```

## Updating Liberty from Version 8.5.0 to Version 8.5.5

Distributed operating systems

IBM i

8.5.5.0

If you are updating an existing WebSphere Application Server Version 8.5.0.x Liberty feature, you must install WebSphere Application Server Liberty Network Deployment Version 8.5.5.0 or later. You cannot make an in-place update of the Version 8.5.0.x Liberty feature. Afterwards, you can copy your data and server configurations to the new installation or, if your user data are kept in another location, follow typical procedures for managing your data and server configurations.

### About this task

In WebSphere Application Server Version 8.5.5.0, Liberty was promoted from a feature to an independently installable offering. You cannot make an in-place update of the Version 8.5.0.x Liberty feature. The `wlp` folder includes the Liberty runtime and any user data or server configurations that you have saved in the `wlp/usr` folder. If you have a combined full-profile and Liberty-profile Version 8.5.0.x installation, the update program will back up the `wlp` folder for the existing Version 8.5.0.x Liberty feature into the `wlp.bak_<timestamp>` folder and uninstall the feature during an update to Version 8.5.5.0 or higher. You can continue using Liberty from the backed-up location or copy it elsewhere. To update Liberty to Version 8.5.5.0 or higher, you then must install WebSphere Application Server Liberty Network Deployment (with the `com.ibm.websphere.liberty.ND.v85` offering ID). After installing WebSphere Application Server Liberty Network Deployment, you can move any user data and server configurations from the `wlp.bak_<timestamp>` folder to the new Liberty installation.

These instructions describe updating from a combined full-profile and Liberty-profile Version 8.5.0.x installation. If you have only the Version 8.5.0.x Liberty feature installed, you should install WebSphere Application Server Liberty Network Deployment Version 8.5.5.0 or higher in a different location. Then, you can copy the contents of the `wlp/usr` directory from the old installation to the `usr` directory of the new installation. If you are using `WLP_USER_DIR` and `WLP_OUTPUT_DIR` environment variables, make sure that they are pointing to the desired locations. You can continue using Java 6 from the Version 8.5.0.x installation image, use your own Java 6 or Java 7 that meets Liberty minimum requirements, or install one or both of the optional Java 6 or Java 7 Liberty extension offerings (offering ids: `com.ibm.websphere.liberty.IMBJAVA.v60` and `com.ibm.websphere.liberty.IMBJAVA.v70`).

**Note:**  During installation of a Liberty offering on an IBM i system, the `WLP_DEFAULT_USER_DIR` and `WLP_DEFAULT_OUTPUT_DIR` environment variables are set in the `WLP_INSTALL_DIR/etc/default.env` file.

## Procedure

1. Update your existing combined full-profile and Liberty-profile installation to Version 8.5.5 or later following the normal update procedure.

**Note:** If you want to keep using the backed-up Liberty with the current level of Java 6 after the update, you must make a backup of Java 6 before it is updated to the latest level by the fix-pack update. Java 6 can be found in the `<install-root>\java` folder. Set the `JAVA_HOME` environment variable to point to the desired Java. For more information on this environment variable, see “Customizing the Liberty environment” on page 1565.

After updating your WebSphere Application Server Network Deployment installation from Version 8.5.0.x to Version 8.5.5, you can find your Liberty installation in the `<was_home>/wlp.bak_<timestamp>` folder. This backup folder contains the Liberty runtime at the level that it was before you started the update.

2. Use the backed-up Liberty runtime.

A copy of the Installation Manager installation and history information for this snapshot is also stored in the root of the backup in the `installed.xml` and `history.xml` files.

To determine what fixes have been installed in this snapshot, you can use the `bin/productInfo` command in the backed-up Liberty folder. See “Liberty:productInfo command” on page 1415 for more information.

You can continue using the Liberty runtime folder from its backed-up location, or you can copy or move it to a new location. If you have set the `WLP_USER_DIR` or `WLP_OUTPUT_DIR` environment variables, make sure that they point to the location of your user data and the location of output resources generated by your server respectively.

**Note:** Do not move the backed-up `wlp.bak_<timestamp>` folder back to `wlp` in case you decide to roll back to Version 8.5.0.x later.

If `WLP_USER_DIR` has not been set, the server configuration and shared resources are stored in the `usr` directory at the root of the server's runtime environment (`wlp_bak_<timestamp>/usr` for example). In this case, no action is required to use the backed-up runtime because the user data can still be found under the `usr` directory of the new location.

If the `WLP_OUTPUT_DIR` value is not set, the default location is in the server root directory (`wlp_bak_<timestamp>/usr/servers/<server_name>` for example). If this environment variable is not set, no action is required to use the backed up runtime because logs continue to appear under the `usr/servers/<server_name>/logs` directory of the new location.

For more information on these environment variables, see “Customizing the Liberty environment” on page 1565.

**Note:** If the `server.xml` file or any included XML configuration file references another resource outside the server configuration directory, ensure that these resources can be found from the new server location.

Start all Liberty servers with the `--clean` parameter as a launch option. For example:

```
server start --clean
```

You need to use the `--clean` option only once. All subsequent server starts will not require it.

If you need to continue using the backed-up Liberty in the `wlp.bak_<timestamp>` folder, you can apply fixes using the archive interim-fix service procedure documented in “Applying an interim fix to a Liberty archive installation” on page 1388.

3. Install WebSphere Application Server Liberty Network Deployment Version 8.5.5 or later.

See “Installing and uninstalling Liberty using Installation Manager” on page 1164 or “Installing and uninstalling Liberty using downloaded files and archives” on page 1371.

**Tip:** After you install WebSphere Application Server Liberty Network Deployment Version 8.5.5 or later, you can use the `ProductInfo compare` action to compare the old and new installations. This will

show any issues that were resolved in the Version 8.5.0.x level that are not resolved at the Version 8.5.5.x level. See “Liberty:productInfo command” on page 1415 for more information.

4. Start using the WebSphere Application Server Liberty Network Deployment Version 8.5.5 installation. If the WLP\_USER\_DIR and WLP\_OUTPUT\_DIR environment variables are set, then the new Liberty installation will continue using these locations to for user data, including server configurations, and to place server generated output. In this case, it is recommended that you make a backup of the directories referenced by WLP\_USER\_DIR and WLP\_OUTPUT\_DIR before beginning to use the new installation.

If the WLP\_USER\_DIR and WLP\_OUTPUT\_DIR environment variables are not set, Liberty will use folders relative to the installed runtime by default. In this case, you should copy the contents of the backed-up Liberty runtime user folder (`wlp.bak_<timestamp>/usr`) to the `usr` folder of your new installation.

For more information on these environment variables, see “Customizing the Liberty environment” on page 1565.

**Note:** If the `server.xml` file or any included XML configuration file references another resource outside the server configuration directory, ensure that these resources can be found from the new server location.

## Installing the Extended Programming Models on IBM i

IBM i

8.5.5.4

Installing and updating Liberty with the Extended Programming Models differs depending on the version of WebSphere Application Server.

### About this task

The Extended Programming Models provide a rich set of programming models such as web services, JMS (including Message-driven beans), and MongoDB 2.0.

How you install the Extended Programming Models depends on your version of WebSphere Application Server:

- Up to Version 8.5.5.3: Extended Programming Models are available as the `extprogmodels` Installation Manager installable feature.
- Version 8.5.5.4 and later: Extended Programming Models are available as the `extendedPackage-1.0` Liberty Repository add-on

You can use the following options to install the Extended Programming Models when you install Liberty or to update an existing copy of Liberty to include the Extended Programming Models:

- Install or update Liberty with the Extended Programming Models using the command line.
- Install or update Liberty with the Extended Programming Models using response files.

**Note:** If you are installing or updating to Version 8.5.5.3 or earlier using a remote repository, such as IBM Passport Advantage or a centrally-hosted HTTP server, internet access is required to update the Extended Programming Models.

After you install Liberty Version 8.5.5.4 or later, you can later install the `extendedPackage-1.0` add-on by using the **featureManager** command. For Version 8.5.5.6 and later, you can also use the **installUtility** command to install the add-on from multiple types of repositories. For more information, see “Installing assets using the featureManager command” on page 1403 and “Installing assets using the installUtility command” on page 1393.

## Procedure

Use one of the following options to install the Extended Programming Models:

- Install or update Liberty with the Extended Programming Models using the command line.
  - V8.5.5.3 and previous versions install the `extprogmodels` feature after the product:

```
imcl install com.ibm.websphere.liberty.ND.v85,extprogmodels
-installationDirectory /QIBM/ProdData/WebSphere/AppServer/V85/ND -acceptLicense
-repositories https://downloads.mycorp.com:8080/WAS_85_repository
-sharedResourcesDirectory /QIBM/UserData/InstallationManager/IMShared
-showProgress
```
  - V8.5.5.4 and later versions install the `extendedPackage-1.0` addon on the `-properties user.addon` parameter:

```
imcl install com.ibm.websphere.liberty.ND.v85
-properties user.accept.license=true,user.addon=extendedPackage-1.0
-installationDirectory /QIBM/ProdData/WebSphere/AppServer/V85/ND -acceptLicense
-repositories https://downloads.mycorp.com:8080/WAS_85_repository
-sharedResourcesDirectory /QIBM/UserData/InstallationManager/IMShared
-showProgress
```
- Install or update Liberty with the Extended Programming Models using response files.
  - V8.5.5.3 and previous versions install the `extprogmodels` feature on the feature attribute of the offering element:

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <variables>
    <variable name='sharedLocation' value='/QIBM/UserData/InstallationManager/IMShared' />
  </variables>
  <server>
    <repository location='http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85' />
  </server>
  <profile id='WebSphere Liberty V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
    <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/ND' />
    <data key='user.import.profile' value='false' />
  </profile>
  <install modify='false'>
    <!-- Install the IBM WebSphere Application Server Network Deployment 8.5.5.0 Liberty with the Extended Programming Models-->
    <offering profile='WebSphere Liberty V8.5' id='com.ibm.websphere.liberty.ND.v85' features='liberty,extprogmodels' installFixes='none' />
  </install>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='${sharedLocation}' />
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45' />
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
  <preference name='offering.service.repositories.areUsed' value='false' />
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
  <preference name='http.ntlm.auth.kind' value='NTLM' />
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
  <preference name='PassportAdvantageIsEnabled' value='false' />
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false' />
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true' />
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true' />
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true' />
</agent-input>
```

- V8.5.5.4 and later versions install the `extendedPackage-1.0` addon on the `user.addon` parameter under the profile element:

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <variables>
    <variable name='sharedLocation' value='/QIBM/UserData/InstallationManager/IMShared' />
  </variables>
  <server>
    <repository location='http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85' />
  </server>
  <profile id='WebSphere Liberty V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
    <data key='eclipseLocation' value='/QIBM/ProdData/WebSphere/AppServer/V85/ND' />
    <data key='user.import.profile' value='false' />
    <!-- Extended Programming Model addon -->
    <data key='user.addon' value='com.ibm.websphere.appserver.extendedPackage-1.0' />
    <data key='user.accept.license' value='true' />
  </profile>
  <install modify='false'>
    <!-- IBM WebSphere Application Server Network Deployment 8.5.5.4 Liberty -->
```

```

    <offering profile='WebSphere Liberty V8.5' id='com.ibm.websphere.liberty.ND.v85' features='liberty' installFixes='none' />
  </install>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='${sharedLocation}' />
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45' />
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
  <preference name='offering.service.repositories.areUsed' value='false' />
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
  <preference name='http.ntlm.auth.kind' value='NTLM' />
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
  <preference name='PassportAdvantageIsEnabled' value='false' />
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false' />
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true' />
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true' />
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true' />
</agent-input>

```

## Adding and removing features from Liberty on IBM i operating systems using response files

### 8.5.5.0

You can install and remove WebSphere Application Server Liberty Network Deployment features using Installation Manager response files.

### About this task

Perform this procedure to use Installation Manager to install or remove a feature silently using a response file.

Like other Installation Manager operations, you can invoke a modification using the **imcl** command-line tool. Go to the IBM Installation Manager Information Center for more information.

#### 8.5.5.4

To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

**Optional features:** In the following list of optional features, the names to be used in the response files are enclosed in parentheses:

- Embeddable EJB container and JPA client (`embeddablecontainer`)

This option installs the embeddable EJB container and JPA client.

The embeddable EJB container is a Java Archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition (SE) environment. You can run enterprise beans using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.

The JPA client can be used with the embeddable EJB container to provide Java Persistence API capability in a Java SE environment.

- Extended Programming Models (`extprogmodels`) - Versions 8.5.5.0 to 8.5.5.3

The Extended Programming Models feature provides a rich set of programming models such as Web Services, JMS (including Message-Driven Beans), and MongoDB 2.0.



#### 8.5.5.4

Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` addon, or install the individual features that you need from the Liberty Repository. See the following topics for more information:

- Installing Liberty Repository assets
- Liberty features

**Note:** To install assets from the IBM WebSphere Liberty Repository, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later.

## Procedure

1. Optional: If the repository requires a username and password, create a credential-storage file to access this repository.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the `-keyring` and `-password` options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the `-secureStorageFile` and `-masterPasswordFile` options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the `-keyring` and `-password` options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

2. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
3. On a CL command line, run the `STRQSH` command to start the Qshell command shell.
4. Use a response file to install or remove a feature.

Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and modify the product. For example:

```
./imcl
input $HOME/WASFiles/temp/modify_response_file.xml
-log $HOME/WASFiles/temp/modify_log.xml
-secureStorageFile $HOME/WASFiles/temp/credential.store -masterPasswordFile $HOME/WASFiles/master_password_file.txt
```

**Note:** The program might write important post-installation instructions to standard output.

For more information on using Installation Manager, read the IBM Installation Manager Information Center.

## Example

- Here are examples of response files for modifying the features in an installation:
  - Here is a response file that adds the Embeddable EJB container and JPA client to an existing product that is installed in the `/QIBM/ProdData/WebSphere/AppServer/V85/ND` directory:

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85' />
</server>
<profile id='WebSphere Liberty V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/ND' />
</profile>
<install modify='true'>
  <offering profile='WebSphere Liberty V8.5' features='embeddablecontainer' id='com.ibm.websphere.liberty.ND.v85' />
</install>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared' />
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
<preference name='offering.service.repositories.areUsed' value='true' />
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
<preference name='http.ntlm.auth.kind' value='NTLM' />
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
<preference name='PassportAdvantageIsEnabled' value='false' />
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
</agent-input>
```

- To alter this response file to remove a feature, simply change the `install` tags to `uninstall`. Here is the same response file modified to remove the Embeddable EJB container and JPA client:

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85' />
```

```

</server>
<profile id='WebSphere Liberty V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/ND' />
</profile>
<uninstall modify='true'>
  <offering profile='WebSphere Liberty V8.5' features='embeddablecontainer' id='com.ibm.websphere.liberty.ND.v85' />
</uninstall>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared' />
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
<preference name='offering.service.repositories.areUsed' value='true' />
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
<preference name='http.ntlm.auth.kind' value='NTLM' />
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
<preference name='PassportAdvantageIsEnabled' value='false' />
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
</agent-input>

```

- To combine adding and removing features using a single response file, add both an install action and an uninstall action.

- Here is an example of the **imcl** command for modifying the features in an installation:

```

./imcl modify com.ibm.websphere.liberty.ND.v85
-addFeatures embeddablecontainer
-repositories http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85
-installationDirectory /QIBM/ProdData/WebSphere/AppServer/V85/ND
-secureStorageFile /var/credential.store -masterPasswordFile /var/master_password_file.txt

```

## Uninstalling Liberty from IBM i operating systems using the command line

**8.5.5.0**

You can use Installation Manager to uninstall WebSphere Application Server Liberty Network Deployment using the Installation Manager command line (**imcl**).

### Procedure

1. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
2. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
3. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
4. Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager.
5. Use the **imcl** command to uninstall the product.

For example:

```

./imcl uninstall com.ibm.websphere.liberty.ND.v85,optional_feature_ID
-installationDirectory installation_directory

```

You can remove a list of features that are separated by commas. If a list of features is not specified, the entire product is uninstalled.

For more information on using the **imcl** command to uninstall the product, see the IBM Installation Manager Information Center.

6. Optional: Uninstall IBM Installation Manager.

**Important:** Before you can uninstall IBM Installation Manager, you must uninstall all of the packages that were installed by Installation Manager.

For more information on uninstalling Installation Manager, see the IBM Installation Manager Information Center.

### Example

Here is an example of using the **imcl** command to uninstall Websphere Application Server:

```

./imcl uninstall com.ibm.websphere.liberty.ND.v85
-installationDirectory /QIBM/ProdData/WebSphere/AppServer/V85/ND

```

## Uninstalling Liberty from IBM i operating systems using response files

8.5.5.0

You can uninstall WebSphere Application Server Liberty Network Deployment using Installation Manager response files.

### About this task

Using Installation Manager, you can work with response files to uninstall the product.

### Procedure

1. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
2. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
3. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
4. Use a response file to uninstall the product.

From a command line on each of the systems from which you want to uninstall the product, change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager and use a response file that you created to uninstall the product. For example:

```
./imcl  
input $HOME/WASFiles/temp/uninstall_response_file.xml  
-log $HOME/WASFiles/temp/uninstall_Tog.xml
```

Here is an example of what the response file might contain:

```
<agent-input>  
<uninstall>  
<offering profile="WebSphere Liberty V8.5"/>  
</uninstall>  
</agent-input>
```

Go to the IBM Installation Manager Information Center for more information.

5. Optional: Uninstall IBM Installation Manager.

**Important:** Before you can uninstall IBM Installation Manager, you must uninstall all of the packages that were installed by Installation Manager.

Read the IBM Installation Manager Information Center for information about using the uninstall script to perform this procedure.

## Installing Liberty interim fixes on IBM i operating systems using the command line

8.5.5.0

Fix packs contain bundled service to bring WebSphere Application Server Liberty for IBM i up to a new level. Interim fixes provide corrective service for specific known problems. You can use the IBM Installation Manager command-line function to update the offering with the fixes that are available for your service level of WebSphere Application Server Liberty for IBM i.

### Before you begin

Contact the IBM Software Support Center for information about updates for WebSphere Application Server Liberty for IBM i. The most current information is available from the IBM Software Support Center and Fix Central.

IBM Installation Manager is used to apply maintenance to WebSphere Application Server Liberty for IBM i.

## About this task

Use this procedure whenever you want to apply a new interim fix to your system.

**Tip:** You can also install interim fixes using silent response files with Installation Manager. For information on creating and using response files, read the IBM Installation Manager Information Center.

**Restriction:** You cannot use the `iRemoteInstall` command to install an interim fix.

## Procedure

1. For a list of interim fixes that are available for WebSphere Application Server Liberty for IBM i and specific information about each interim fix, perform the following actions.
  - a. Go to Fix Central.
  - b. Select **WebSphere** as the product group.
  - c. Select **WebSphere Application Server Liberty for IBM i** as the product.
  - d. Select the version of the offering to be updated.
  - e. Select your operating system as the platform, and click **Continue**.
  - f. Select **Browse for fixes**, and click **Continue**.
  - g. Click **More Information** under each fix to view information about the fix.
  - h. **Recommendation:** Make a list of the names of the interim fixes that you would like to install.

2. Update WebSphere Application Server Liberty for IBM i with the interim fixes using one of the following procedures.

- **Access the live service repository that contains the fixes, and use web-based updating.**

Use Installation Manager on your local system to update WebSphere Application Server Liberty for IBM i with the interim fixes from the live web-based service repositories.

- For the live service repositories, use the same URLs as those used for the generally available product-offering repositories during installation. These URLs are listed in Online product repositories for WebSphere Application Server offerings.
- These locations do not contain web pages that you can access using a web browser. They are remote web-based repository locations that you specify for Installation Manager so that it can maintain the offering.

To install an interim fix from a service repository, perform the following actions:

- a. If you do not already have Installation Manager credential-storage and master-password files containing your IBM software user ID and password, create files that will allow you to access the repository.

**Note:** These are the credentials that you use to access protected IBM software websites.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

- b. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
- c. Stop all servers and applications on the WebSphere Application Server Liberty for IBM i installation that is being updated.
- d. On a CL command line, run the STRQSH command to start the Qshell command shell.
- e. Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

To set the umask setting to 022, issue the following command:

```
umask 022
```

- f. Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager. On IBM i systems, the root directory for the Installation Manager is */QIBM/ProdData/InstallationManager*.

- g. Install the interim fix.

```
./imcl install interim_fix_name
  -installationDirectory offering_installation_location
  -repositories repository_URL
  -secureStorageFile storage_file -masterPasswordFile master_password_file
```

- h. **Optional:** List all installed packages to verify the installation:

```
./imcl listInstalledPackages -long
```

- **Download the files that contain the fixes from Fix Central, and use local updating.**

You can download compressed files that contain the fixes from Fix Central. Each compressed fix file contains an Installation Manager repository for the fix and usually has a .zip extension. After downloading the fix files, you can use Installation Manager to update WebSphere Application Server Liberty for IBM i with the interim fixes.

- a. To download the interim fixes, perform the following actions:

- 1) Go to Fix Central.
- 2) Select **WebSphere** as the product group.
- 3) Select **WebSphere Application Server Liberty for IBM i** as the product.
- 4) Select the version of the offering to be updated.
- 5) Select your operating system as the platform, and click **Continue**.
- 6) Select **Browse for fixes**, and click **Continue**.
- 7) Select the interim fixes that you want to download, and click **Continue**.
- 8) Select your download options, and click **Continue**.
- 9) Click **I agree** to agree to the terms and conditions.
- 10) Click **Download now** to download the interim fixes.
- 11) Transfer the compressed fix files in binary format to the IBM i system on which they will be installed.

- b. To install an interim fix from a downloaded file, perform the following actions:

- 1) Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
- 2) Stop all servers and applications on the WebSphere Application Server Liberty for IBM i installation that is being updated.
- 3) On a CL command line, run the STRQSH command to start the Qshell command shell.
- 4) Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

To set the umask setting to 022, issue the following command:

```
umask 022
```

- 5) Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager.

On IBM i systems, the root directory for the Installation Manager is */QIBM/ProdData/InstallationManager*.

- 6) Install the interim fix.

```
./imcl install interim_fix_name  
-installationDirectory offering_installation_location  
-repositories compressed_file
```

- 7) **Optional:** List all installed packages to verify the installation:

```
./imcl listInstalledPackages -long
```

## Installing Liberty fix packs on IBM i operating systems using the command line

8.5.5.0

Product fix packs contain bundled service to bring WebSphere Application Server Liberty Network Deployment up to a new product level. Interim fixes provide corrective service for specific known problems. You can use the IBM Installation Manager command-line function to update the product with the fixes that are available for your service level of WebSphere Application Server Liberty Network Deployment installation.

### Before you begin

Contact the IBM Software Support Center for information about updates for WebSphere Application Server for IBM i. The most current information is available from the IBM Software Support Center and Fix Central.



8.5.5.6

If you want to install Liberty assets from local directory-based repositories or an instance of the Liberty Asset Repository Service, configure the repositories. For more information about the Liberty asset repositories, see “Installing assets using Installation Manager” on page 1411.

**Tip:** As an alternative to the procedure that is described in this article, Installation Manager allows you to use the **updateAll** command in a response file or on the command line to search for and update all installed packages. Use this command only if you have full control over which fixes are contained in the targeted repositories. If you create and point to a set of custom repositories that include only the specific fixes that you want to install, you should be able to use this command confidently. If you enable searching service repositories or install fixes directly from other live web-based repositories, then you might not want to select this option so that you can select only the fixes that you want to install using the **-installFixes** option with the **install** command on the command line or the **installFixes** attribute in a response file.

### About this task

**New:** Fix pack 16.0.0.2 is the next fix pack after 8.5.5.9. You can continue to use the same Version 8.5 Installation Manager repositories and offering IDs to install or update to 16.0.0.2, or you can use the new versionless repositories and offerings. For more information about fix pack 16.0.0.2, see What is new in Liberty in the new location of the latest Liberty documentation.

- You can also install fix packs using response files with Installation Manager. For information on creating and using response files, read “Installing Liberty fix packs on IBM i operating systems using response files” on page 1323 and the IBM Installation Manager Information Center.
- You cannot use the `iRemoteInstall` command to install a fix pack.

- **8.5.5.4** To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

## Procedure

1. For a list of fixes that are available for WebSphere Application Server Liberty Network Deployment installation and specific information about each fix, perform the following actions.
  - a. Go to Fix Central.
  - b. Select **WebSphere** as the product group.
  - c. Select **WebSphere Application Server** as the product.
  - d. Select the installed version.
  - e. Select your operating system as the platform, and click **Continue**.
  - f. Select **Browse for fixes**, and click **Continue**.
  - g. Click **More Information** under each fix to view information about the fix.
  - h. **Recommendation:** Make a list of the names of the fixes that you would like to install.
2. Update WebSphere Application Server Liberty Network Deployment installation with the fix pack using one of the following procedures.

- Access the live service repository that contains the fix pack, and use web-based updating.

Use Installation Manager on your local system to update WebSphere Application Server Liberty Network Deployment with the interim fixes from the live web-based service repositories.

- For the live service repositories, use the same URLs as those used for the generally available product-offering repositories during installation. These URLs are based on the following pattern:  
`http://www.ibm.com/software/repositorymanager/offering_ID`

where *offering\_ID* is the offering ID that you can find in WebSphere Application Server product offerings for supported operating systems.

- These locations do not contain web pages that you can access using a web browser. They are remote web-based repository locations that you specify for Installation Manager so that it can maintain the product.

To install a fix from a service repository, perform the following actions:

- a. If you do not already have Installation Manager credential-storage and master-password files containing your IBM software user ID and password, create files that will allow you to access the repository.

**Note:** These are the credentials that you use to access protected IBM software websites. For information on creating credential-storage and master-password files for Installation Manager, read the IBM Installation Manager Information Center.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the `imutilsc` command is unable to find the URL that is specified.

- b. Sign on to the IBM i system with a user profile that has `*ALLOBJ` and `*SECADM` special authorities.
- c. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being updated.
- d. On a CL command line, run the STRQSH command to start the Qshell command shell.
- e. Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

To set the umask setting to 022, issue the following command:

```
umask 022
```

- f. Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager. On IBM i systems, the root directory for the Installation Manager is */QIBM/ProdData/InstallationManager*.
- g. Install the fix pack.

```
./imcl install offering_ID_offering_version,optional_feature_ID
-repositories source_repository
-installationDirectory offering_installation_location
-secureStorageFile storage_file -masterPasswordFile master_password_file
-acceptLicense
```

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

#### Tips:

- The *offering\_ID* is the offering ID that is listed in WebSphere Application Server product offerings for supported operating systems.
- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.5.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
./imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the **-installFixes** argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the **-installFixes** option defaults to all.
  - If the offering version is specified, the **-installFixes** option defaults to none.
- You can add a list of features that are separated by commas.

-  **8.5.5.2** You can specify additional assets to install from the Liberty Repository. For a list of Liberty Repository assets, see the downloads page on WASdev.net.

To install assets from the IBM WebSphere Liberty Repository, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later.

If you want to install Liberty Repository features, specify the short names or symbolic names on the **user.feature** option of the **-properties** parameter. Multiple feature names are separated with double commas. The following example installs the Portlet Container and Portlet Serving features:

```
-properties user.feature=portlet-2.0,,portletserving-2.0,user.accept.license=true
```

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.

**8.5.5.4**

Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` addon, or install the individual features that you need from the Liberty Repository. See the following topics for more information:

- Installing Liberty Repository assets
- Liberty features

You can install the complete set of Extended Programming Model features by specifying the `user.addon` option:

```
-properties user.addon=extendedPackage-1.0,user.acceptLicense=true
```

If you upgrade WebSphere Application Server Liberty Version 8.5.5.3 or previous versions that contain the `extprogmodels` feature, Installation Manager automatically installs the `extendedPackage-1.0` add-on. You must specify the `user.acceptLicense` option:

```
-properties user.acceptLicense=true
```

**8.5.5.6**

You can also install assets from instances of the Liberty Asset Repository Service or local directory-based repositories. For more information about these asset repositories, see “Installing assets using Installation Manager” on page 1411. Add the repository on the `-repositories` parameter. The repositories are accessed in the order that they are specified. By default, the Liberty Repository is the last of the repositories that are accessed during installation. To disable access to the Liberty Repository, on the `-properties` parameter, set the `user.useLibertyRepository` option to `false`.

**8.5.5.8**

```
./imcl install com.ibm.websphere.liberty.ND.v85
-properties user.useLibertyRepository=false,user.addon=extendedPackage-1.0,user.feature=portlet-2.0
-installationDirectory /QIBM/ProdData/Liberty -acceptLicense
-repositories /QIBM/LibertyProductRepo,https://your_onprem_asset_repo_url,/QIBM/LocalAssetRepo,/QIBM/LocalAssetRepo2.zip
-sharedResourcesDirectory /QIBM/UserData/InstallationManager/IMShared
-showProgress
```

To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.

- If you obtained the fix pack by installing the WebSphere Application Server group PTF, you can use the local fix-pack repositories to install the fix pack.

For information about the local fix-pack repositories, see file `/QIBM/WAS/WASFixpacks/ReadmeV85.html` or `/QIBM/WAS/WASFixpacks/ReadmeV85.txt`.

h. **Optional:** List all installed packages to verify the installation:

```
./imcl listInstalledPackages -long
```

- Download a file that contains the fix pack from Fix Central, and use local updating.

You can download a compressed file that contains the fix pack from Fix Central. Each compressed fix file contains an Installation Manager repository for the fix pack and usually has a `.zip` extension. After downloading the fix file, you can use Installation Manager to update WebSphere Application Server LibertyNetwork Deployment with the fix pack.

a. To download the fix pack, perform the following actions:

- 1) Go to Fix Central.
- 2) Select **WebSphere** as the product group.
- 3) Select **WebSphere Application Server** as the product.
- 4) Select the installed version.
- 5) Select your operating system as the platform, and click **Continue**.
- 6) Select **Browse for fixes**, and click **Continue**.
- 7) Select the fix pack that you want to download, and click **Continue**.
- 8) Select your download options, and click **Continue**.
- 9) Click **I agree** to agree to the terms and conditions.
- 10) Click **Download now** to download the fix pack.

- 11) Transfer the compressed fix file in binary format to the IBM i systems on which it will be installed.
  - 12) Extract the compressed repository file to a directory on your system.
- b. To install a fix pack from a downloaded file, perform the following actions:
- 1) Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
  - 2) Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation that is being updated.
  - 3) On a CL command line, run the STRQSH command to start the Qshell command shell.
  - 4) Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

To set the umask setting to 022, issue the following command:

```
umask 022
```

- 5) Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager.

On IBM i systems, the root directory for the Installation Manager is /QIBM/ProdData/InstallationManager.

- 6) Install the fix pack.

```
./imcl install offering_ID_offering_version,optional_feature_ID
-repositories location_of_expanded_files
-installationDirectory offering_installation_location
-acceptLicense
```

#### Tips:

- The *offering\_ID* is the offering ID that is listed in WebSphere Application Server product offerings for supported operating systems.
- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.5.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
./imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the *-installFixes* argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the *-installFixes* option defaults to all.
  - If the offering version is specified, the *-installFixes* option defaults to none.
- You can add a list of features that are separated by commas.
- You can specify additional assets to install from the Liberty Repository. For a list of Liberty Repository assets, see the downloads page on WASdev.net.

To install assets from the IBM WebSphere Liberty Repository, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later.

If you want to install Liberty Repository features, specify the short names or symbolic names on the **user.feature** option of the **-properties** parameter. Multiple feature names are separated with double commas. The following example installs the Portlet Container and Portlet Serving features:

```
-properties user.feature=portlet-2.0,,portletserving-2.0,user.accept.license=true
```

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.



**8.5.5.4** Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` addon, or install the individual features that you need from the Liberty Repository. See the following topics for more information:

- Installing Liberty Repository assets
- Liberty features

You can install the complete set of Extended Programming Model features by specifying the **user.addon** option:

```
-properties user.addon=extendedPackage-1.0,user.accept.license=true
```

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.

If you upgrade WebSphere Application Server Liberty Version 8.5.5.3 or previous versions that contain the `extprogmodels` feature, Installation Manager automatically installs the `extendedPackage-1.0` add-on. You must specify the **user.accept.license** option:

```
-properties user.accept.license=true
```



**8.5.5.6** You can also install assets from instances of the Liberty Asset Repository Service or local directory-based repositories. For more information about these asset repositories, see “Installing assets using Installation Manager” on page 1411. Add the repository on the **-repositories** parameter. The repositories are accessed in the order that they are specified. By default, the Liberty Repository is the last of the repositories that are accessed during installation. To disable access to the Liberty Repository, on the **-properties** parameter, set the **user.useLibertyRepository** option to `false`. **8.5.5.8**

```
imcl install com.ibm.websphere.liberty.nd.v85
-properties user.useLibertyRepository=false,user.addon=extendedPackage-1.0,user.feature=portlet-2.0
-installationDirectory D:\IBM\Liberty -acceptLicense
-repositories D:\IBM\LibertyProductRepo,https://your_onprem_asset_repo_url,D:\IBM\LocalAssetRepo,D:\IBM\LocalAssetRepo2.zip
-sharedResourcesDirectory D:\IBM\IMShared
-showProgress
```

To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.

- If you obtained the fix pack by installing the WebSphere Application Server group PTF, you can use the local fix-pack repositories to install the fix pack.

For information about the local fix-pack repositories, see file `/QIBM/WAS/WASFixpacks/ReadmeV85.html` or `/QIBM/WAS/WASFixpacks/ReadmeV85.txt`.

- 7) **Optional:** List all installed packages to verify the installation:

```
./imcl listInstalledPackages -long
```

## Installing Liberty fix packs on IBM i operating systems using response files

**8.5.5.0**

You can update WebSphere Application Server Liberty Network Deployment to a later version using Installation Manager response files.

## Before you begin



8.5.5.6

If you want to install Liberty assets from local directory-based repositories or an instance of the Liberty Asset Repository Service, configure the repositories. For more information about the Liberty asset repositories, see “Installing assets using Installation Manager” on page 1411.

**Tip:** As an alternative to the procedure that is described in this article, Installation Manager allows you to use the **updateAll** command in a response file or on the command line to search for and update all installed packages. Use this command only if you have full control over which fixes are contained in the targeted repositories. If you create and point to a set of custom repositories that include only the specific fixes that you want to install, you should be able to use this command confidently. If you enable searching service repositories or install fixes directly from other live web-based repositories, then you might not want to select this option so that you can select only the fixes that you want to install using the **-installFixes** option with the **install** command on the command line or the **installFixes** attribute in a response file.

## About this task

- | **New:** Fix pack 16.0.0.2 is the next fix pack after 8.5.5.9. You can continue to use the same Version 8.5
- | Installation Manager repositories and offering IDs to install or update to 16.0.0.2, or you can use the new
- | versionless repositories and offerings. For more information about fix pack 16.0.0.2, see What is new in
- | Liberty in the new location of the latest Liberty documentation.

8.5.5.4

To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

## Procedure

1. Optional: If the repository requires a username and password, create a credential-storage file to access this repository.

**Tip:** When creating a credential-storage file, append `/repository.config` at the end of the repository URL location if the **imutilsc** command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

2. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
3. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
4. Use a response file to update the product.

Change to the `eclipse/tools` subdirectory in the directory where you installed Installation Manager, and update the product. For example:

```
./imcl -acceptLicense  
input $HOME/WASFiles/temp/update_response_file.xml  
-log $HOME/WASFiles/temp/update_log.xml  
-secureStorageFile $HOME/WASFiles/temp/credential.store -masterPasswordFile $HOME/WASFiles/master_password_file.txt
```

**Note:** The program might write important post-installation instructions to standard output.

For more information on using Installation Manager, read the IBM Installation Manager Information Center.

## Example

The following is an example of a response file for updating WebSphere Application Server LibertyNetwork Deployment to a later version.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85' />
</server>
<profile id='WebSphere Liberty V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
  <data key='was.install.os400.profile.location' value='/QIBM/UserData/WebSphere/AppServer/V85/ND' />
</profile>
<install modify='false'>
  <offering profile='WebSphere Liberty V8.5' id='com.ibm.websphere.liberty.ND.v85'
    version='8.5.5.20101025_2108' />
</install>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/QIBM/UserData/InstallationManager/IMShared' />
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
<preference name='offering.service.repositories.areUsed' value='true' />
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
<preference name='http.ntlm.auth.kind' value='NTLM' />
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
<preference name='PassportAdvantageIsEnabled' value='false' />
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
</agent-input>
```

### Tips:

- The profile ID (`<profile . . . id='profile_ID' . . . >` and `<offering . . . profile='profile_ID' . . . >`) can be found when you run the `imcl listInstallationDirectories -verbose` command from the `eclipse/tools` subdirectory in the directory where you installed Installation Manager. It is the same as the package group's name.
- The *version* is a specific version of the offering to install (8.5.5.20101025\_2108 for example). This specification is optional.
  - If *version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If *version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
./imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the `-installFixes` option defaults to all.
  - If the offering version is specified, the `-installFixes` option defaults to none.
- If you obtained the fix pack by installing the WebSphere Application Server group PTF, you can use the local fix-pack repositories to install the fix pack.

For information about the local fix-pack repositories, see file `/QIBM/WAS/WASFixpacks/ReadmeV8.html` or `/QIBM/WAS/WASFixpacks/ReadmeV8.txt`.

-  **8.5.5.2** You can specify additional assets to install from the Liberty Repository. For a list of Liberty Repository assets, see the downloads page on WASdev.net.

To install Liberty Repository assets, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later. Previous versions of Installation Manager do not have the option to install Liberty Repository assets. If you use a response file and did not update Installation Manager to Version 1.6.2 or later, the assets that you specify in the response file are ignored during installation.

If you want to install additional features, specify two extra data key elements in your response file. You can use either the symbolic name or the short name.

The following example installs the Portlet Container and Portlet Serving features using the symbolic name.

```
<data key='user.feature' value='com.ibm.websphere.appserver.portlet-2.0,,com.ibm.websphere.appserver.portletserving-2.0' />
<data key='user.accept.license' value='true' />
```

The following example installs the Portlet Container and Portlet Serving features using the short name:

```
<data key='user.feature' value='portlet-2.0,,portletserving-2.0' />
<data key='user.accept.license' value='true' />
```

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.



**8.5.5.4**

Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` addon, or install the individual features that you need from the Liberty Repository. See the following topics for more information:

- Installing Liberty Repository assets
- Liberty features

The following example installs the Extended Programming Models using the `user.addon` parameter and the Portlet Container and Portlet Serving features using the `user.feature` parameter with short names:

```
<data key='user.addon' value='extendedPackage-1.0' />
<data key='user.feature' value='portlet-2.0,,portletserving-2.0' />
<data key='user.accept.license' value='true' />
```



**8.5.5.6**

You can also install assets from an instance of the Liberty Asset Repository Service or local directory-based repositories. For more information, see “Installing assets using Installation Manager” on page 1411. Add the repository on `repository` elements. If Installation Manager does not recognize the repository, point directly to the `repository.config` file. When you install assets, the repositories are accessed in the order that you specify them.

```
<server>
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85" />
<repository location="https://your_onprem_asset_repo_url" />
<repository location="/QIBM/LocalAssetRepo" />
```

**8.5.5.8**

`<repository location="/QIBM/LocalAssetRepo2.zip" /> </server>` By default, the Liberty Repository is the last of the repositories that are accessed during installation. To disable access to the Liberty Repository, set the `user.useLibertyRepository` parameter to `false`:

```
<data key='user.addon' value='extendedPackage-1.0' />
<data key='user.feature' value='portlet-2.0,,portletserving-2.0' />
<data key='user.useLibertyRepository' value='false' />
```

To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.

•

**Note:** **8.5.5.3** If you are updating to Version 8.5.5.3 and previously installed Liberty Repository features but do not currently have a connection to the IBM WebSphere Liberty Repository, you cannot update using a response file. Instead, update the product by running the `imcl` command and specifying the `user.feature=""` parameter.

## Uninstalling Liberty interim fixes from IBM i operating systems using the command line

**8.5.5.0**

You can use the IBM Installation Manager command-line function to remove interim fixes from WebSphere Application Server Liberty Network Deployment.

## About this task

Use this procedure whenever you want to remove an interim fix from your system using the command line.

**Tip:** You can also uninstall interim fixes using silent response files with Installation Manager. For information on creating and using response files, read “Installing Liberty fix packs on IBM i operating systems using response files” on page 1323 and the IBM Installation Manager Information Center.

## Procedure

1. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
2. Stop all servers and applications on the WebSphere Application Server Liberty Network Deployment installation.
3. On a CL command line, run the STRQSH command to start the Qshell command shell.
4. Make sure that the umask is set to 022.

To verify the umask setting, issue the following command:

```
umask
```

To set the umask setting to 022, issue the following command:

```
umask 022
```

5. Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager. On IBM i systems, the root directory for the Installation Manager is */QIBM/ProdData/InstallationManager*.

6. Uninstall the interim fix:

```
./imcl uninstall interim_fix_name  
-installationDirectory offering_installation_location
```

7. Optional: List all installed packages to verify the uninstallation.

```
./imcl listInstalledPackages -long
```

## Uninstalling Liberty fix packs from IBM i operating systems using the command line

8.5.5.0

You can roll back WebSphere Application Server Liberty Network Deployment to an earlier version using the Installation Manager command line.

### Before you begin

**Restriction:** In order to use this procedure, you must have Installation Manager Version 1.6 or later installed on your system.

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your computer when you install a package. If you change the default setting or delete the saved files, Installation Manager requires access to the repository that was used to install the earlier version.

**Note:** In WebSphere Application Server Version 8.5.5.0, Liberty was promoted from a feature to an independently installable offering. After updating to WebSphere Application Server Liberty Network Deployment Version 8.5.5.x from Version 8.5.0.x, you can roll back to the Version 8.5.0.x Liberty feature level that you were at before updating. If you previously had a combined full-profile and Liberty-profile installation, the Liberty feature will be reinstalled to the wlp folder when you roll back. Any user data and server configurations will not be restored. If necessary, you can copy them from the backed-up

location into the new wlp/usr folder after rollback. If any wlp.bak\_<timestamp> directories are present in your installation image, they will not be affected by the rollback. If you update and roll back multiple times between Version 8.5.0.x and Version 8.5.5.x levels, therefore, you will have multiple wlp.bak\_<timestamp> folders in your installation image. These can always be deleted, copied, or moved without negative impact to your installation.

## Procedure

1. Optional: If the repository requires a username and password, create a credential-storage file to access this repository.

**Tip:** When creating a credential-storage file, append /repository.config at the end of the repository URL location if the **imutilsc** command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

2. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
3. Stop all servers and applications on the installation that is being rolled back.
4. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
5. Change to the eclipse/tools subdirectory in the directory where you installed Installation Manager.
6. Use the **imcl** command to roll back the product.

```
./imcl rollback offering_ID offering_version
  -repositories source_repository
  -installationDirectory installation_directory
  -preferences preference_key=value
  -properties property_key=value
  -secureStorageFile storage_file -masterPasswordFile master_password_file
  -acceptLicense
```

### Tips:

- The *offering\_ID* is the offering ID that is listed in WebSphere Application Server product offerings for supported operating systems.
- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to which to roll back (8.5.5.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the installation rolls back to the previously installed version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the installation rolls back to the specified earlier version of the offering and **no** interim fixes for that version are installed.
- If you previously installed Liberty Repository features and addons but do not have access to a Liberty repository when you rollback your installation, specify the following properties in the response file:

```
-properties user.addon="",user.feature=""
```

Specifying these properties enables the product to rollback and uninstalls all features and addons.

For more information on using the **imcl** command, read the IBM Installation Manager Information Center.

7. Optional: List all installed packages to verify the roll back.

```
./imcl listInstalledPackages -long
```

## Uninstalling Liberty fix packs from IBM i operating systems by using response files

8.5.5.0

You can rollback WebSphere Application Server Liberty Network Deployment to an earlier version by using Installation Manager response files.

### Before you begin

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your computer when you install a package. If you change the default setting or delete the saved files, Installation Manager requires access to the repository that was used to install the earlier version.

**Note:** In WebSphere Application Server Version 8.5.5.0, Liberty was promoted from a feature to an independently installable offering. After updating to WebSphere Application Server Liberty Network Deployment Version 8.5.5.x from Version 8.5.0.x, you can rollback to the Version 8.5.0.x Liberty feature level that you were at before updating. If you previously had a combined full-profile and Liberty-profile installation, the Liberty feature will be reinstalled to the wlp folder when you rollback. Any user data and server configurations will not be restored. If necessary, you can copy them from the backed-up location into the new wlp/usr folder after rollback. If any wlp.bak\_<timestamp> directories are present in your installation image, they will not be affected by the rollback. If you update and rollback multiple times between Version 8.5.0.x and Version 8.5.5.x levels, therefore, you will have multiple wlp.bak\_<timestamp> folders in your installation image. These can always be deleted, copied, or moved without negative impact to your installation.

### Procedure

1. Optional: If the repository requires a username and password, create a credential-storage file to access this repository.

**Tip:** When creating a credential-storage file, append /repository.config at the end of the repository URL location if the **imutilsc** command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

2. Sign on to the IBM i system with a user profile that has \*ALLOBJ and \*SECADM special authorities.
3. Stop all servers and applications on the installation that is being rolled back.
4. On a CL command line, run the **STRQSH** command to start the Qshell command shell.
5. Use a response file to rollback the product.

Change to the eclipse/tools subdirectory in the directory where you installed Installation Manager, and rollback the product. For example:

```
./imcl
input $HOME/WASFiles/temp/rollback_response_file.xml
-log $HOME/WASFiles/temp/rollback_log.xml
-secureStorageFile $HOME/WASFiles/temp/credential.store -masterPasswordFile $HOME/WASFiles/master_password_file.txt
```

**Note:** The program might write important post-installation instructions to standard output.  
For more information on using Installation Manager, read the IBM Installation Manager Information Center.

6. Optional: List all installed packages to verify the rollback.

```
./imcl listInstalledPackages -long
```

## Example

The following is an example of a response file for rolling back the product to an earlier version.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<server>
  <repository location='https://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85' />
</server>
<profile id='WebSphere Liberty V8.5' installLocation='/QIBM/ProdData/WebSphere/AppServer/V85/ND'>
</profile>
<rollback>
  <offering profile='WebSphere Liberty V8.5' id='com.ibm.websphere.liberty.ND.v85' version='8.5.5.20101025_2108' />
</rollback>
</agent-input>
```

## Tips:

- The profile ID (<profile . . . id='profile\_ID' . . . .> and <offering . . . profile='profile\_ID' . . . .>) can be found when you run the `imcl listInstallationDirectories -verbose` command from the `eclipse/tools` subdirectory in the directory where you installed Installation Manager. It is the same as the package group's name.
- The offering ID (<offering . . . id='offering\_ID' . . . .>) can be found in WebSphere Application Server product offerings for supported operating systems.
- The *version* is a specific version of the offering to which to rollback (8.5.5.20101025\_2108 for example). This specification is optional.
  - If *version* is **not** specified, the installation rolls back to the previously installed version of the offering and **all** interim fixes for that version are installed.
  - If *version* is specified, the installation rolls back to the specified earlier version of the offering and **no** interim fixes for that version are installed.
- If you previously installed Liberty Repository features and addons but do not have access to a Liberty repository when you rollback your installation, specify the following properties in the response file:

```
<data key='user.feature' value='' />
<data key='user.addon' value='' />
```

Specifying these properties enables the product to rollback and uninstalls all features and addons.

## Using the sample response files

You can edit and use sample response files for installing, modifying, or uninstalling IBM Web Enablement Liberty for IBM i silently.

## Procedure

- “Sample response file: Installing IBM Web Enablement Liberty for IBM i”
- “Sample response file: Modifying IBM Web Enablement Liberty for IBM i” on page 1335
- “Sample response file: Uninstalling IBM Web Enablement Liberty for IBM i” on page 1339

## Sample response file: Installing IBM Web Enablement Liberty for IBM i:

You can edit and use this example of a response file for installing IBM Web Enablement Liberty for IBM i.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- ##### Copyright #####
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2013.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
```

```

##### -->

<!-- ##### Frequently Asked Questions #####
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
# Installation Manager Information Center can be found at:
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
# Windows = IBMIM.exe -record c:\temp\responsefiles\WASv85.install.Win32.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
# Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv85.install.RHEL64.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse/tools subdirectory in the directory where you installed
# Installation Manager:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
# Windows = imcl.exe -acceptLicense -showProgress
# input c:\temp\responsefile\WASv85.install.Win32.xml
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input /home/user/responsefile/WASv85.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
# license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help: IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. There are two methods for storing authentication credentials
# for Installation Manager depending on the version being used,
# either key ring files or storage files.
#
# Versions of Installation Manger before 1.6.2 use a key ring file to store
# encrypted credentials for authenticating with repositories. Follow this
# two-step process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
# Windows = IBMIM.exe -keyring <path and file name> -password <password>
# Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
# -password <password>
#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <path and file name of response file>
# -keyring <path and name of key ring file> -password <password>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <path and file name of response file>

```

```

# -keyring <path and name of key ring file> -password <password>
#
# Versions of Installation Manager at 1.6.2 or higher use storage files
# to store encrypted credentials. Complete the following steps to create
# master password and storage files to use with Installation Manager.
#
# First, if you do not have a master password file already, create a text file
# that contains a master passphrase. An example of a passphrase is:
# "This text is the passphrase for a master password file."
#
# Next, run imutilsc under the eclipse/tools subdirectory with the following
# options to create and store user credentials in a storage file.
# -secureStorageFile <path and file name of storage file>
# -masterPasswordFile <path and file name of master password file>
# -url <repository address> or -passportAdvantage <PPA repository address>
# -userName <user name>
# -userPassword <password for user>
#
# Example of a command to create a storage file by operating system
# Windows = imutilsc saveCredential -url http://myServer -userName myUserName
# -userPassword myPassword -secureStorageFile C:\IBM\credential.store
# -masterPasswordFile C:\IBM\master_password_file.txt
# Linux, UNIX, IBM z/OS, and the OS X operating system =
# ./imutilsc saveCredential -url http://myServer -userName myUserName
# -userPassword myPassword -secureStorageFile /home/IBM/credential.store
# -masterPasswordFile /home/user/IBM/master_password_file.txt
#
# Usage hints:
# * Do not use both the -url and -passportAdvantage options in the same command.
# * Enclose file paths that include spaces with double quotation marks.
# * If you use the IBM service repositories, you can specify the value:
# http://www.ibm.com/software/repositorymanager/entitled/repository.xml
# for the -url option which is a generic service repository for IBM packages.
# * Repeat steps to store credentials for multiple users in one file.
# * Repeat steps to store credentials for multiple repositories in one file.
#
# Afterwards, when you start a silent installation, run imcl under the eclipse/tools
# subdirectory, and provide Installation Manager with the location of the storage
# file. For example:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <path and file name of response file>
# -secureStorageFile <path and name of storage file>
# -masterPasswordFile <path and name of master password file>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <path and file name of response file>
# -secureStorageFile <path and name of storage file>
# -masterPasswordFile <path and name of master password file>
#
##### -->

<!-- ##### Agent Input #####
#
# Note that the acceptLicense attribute has been deprecated.
# Use the -acceptLicense command line option to accept license agreements.
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
# true = only use the repositories and other preferences that are
# specified in the response file.
# false = use the repositories and other preferences that are
# specified in the response file and Installation Manager.
#
# Valid values for temporary:
# true = repositories and other preferences specified in the
# response file do not persist in Installation Manager.
# false = repositories and other preferences specified in the
# response file persist in Installation Manager.
#
##### -->

<agent-input clean="true" temporary="true">

<!-- ##### Repositories #####
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.

```

```

#
##### -->

<server>
<!-- ##### IBM WebSphere Live Update Repositories #####
# These repositories contain WebSphere Application Server Liberty offerings,
# and updates for those offerings
#
# To use the secure repository (https), you must have an IBM ID,
# which can be obtained by registering at: http://www.ibm.com/account
# or your Passport Advantage account.
#
# And, you must use a key ring file with your response file.
##### -->
<repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.WEBENAB.v85"/>
<!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

<!-- ##### Custom Repositories #####
# Uncomment and update the repository location key below
# to specify URLs or UNC paths to any intranet repositories
# and directory paths to local repositories to use.
##### -->
<!-- <repository location="https://w3.mycompany.com/repositories"/> -->
<!-- <repository location="/home/user/repositories/websphere"/> -->

<!-- ##### Local Repositories #####
# Uncomment and update the following line when using a local
# repository located on your own machine to install a
# WebSphere Application Server Liberty offering.
##### -->
<!-- <repository location='insert the full directory path inside single quotes' /> -->
</server>

<!-- ##### Install Packages #####
#
# Install Command
#
# Use the install command to inform Installation Manager of the
# installation packages to install.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
# false = indicates not to modify an existing install by adding
# or removing features.
# true = indicates to modify an existing install by adding or
# removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for the WEBENAB
# edition of WebSphere Application Server Liberty.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed at the version level specified
# as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install
# the latest version available in the repositories. The version number
# can be found in the repository.xml file in the repositories.
# For example, <offering ... version='8.5.5000.20130326_0211'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of WebSphere Application Server Liberty.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Application Server Liberty include:
# liberty,embeddablecontainer,extprogmodels
#
# The features embeddablecontainer,extprogmodels
# are subfeatures of liberty.
#
# You can use these functions to add or remove feature embeddablecontainer or extprogmodels later.
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
# none = do not install available fixes with the offering.
# recommended = installs all available recommended fixes with the offering.
# all = installs all available fixes with the offering.
#

```

```

# Interim fixes for offerings also can be installed while they
# are being installed by including the offering ID for the interim
# fix and specifying the profile ID.
#
# Installation Manager supports installing multiple offerings at once.
# Additional offerings can be included in the install command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# WebSphere Application Server Liberty as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, installing WebSphere Application Server Liberty Offerings on
# a 64-bit system will require to include one of the options for an IBM Software
# Development Kit, this can be specified by data key cic.selector.arch, its value
# can be either x86 (for 32-bit), or x86_64 (for 64-bit).
#
# More details for cic.selector.arch can be found in the link below:
#
# https://infocenters.hursley.ibm.com/was/vNext/draft/help/index.jsp?topic=%2Fcom.ibm.websphere.wlp.core.doc%2Fae%2Ftwlp_ins_installation_dist_silent.html
#
##### -->

<install modify="false">
<offering id="com.ibm.websphere.liberty.WEBENAB.v85" profile="WebSphere Liberty V8.5" features="liberty,embeddablecontainer,extprogmodels" installFixes="none" />
</install>
<profile id="WebSphere Liberty V8.5" installLocation="/QIBM/ProdData/WebSphere/Liberty/V85/Express">
<data key="eclipseLocation" value="/QIBM/ProdData/WebSphere/Liberty/V85/Express" />
<data key="cic.selector.arch" value="x86_64" />
</profile>

<!-- ##### Shared Data Location #####
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared' />
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r5/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
# true = store downloaded artifacts in the shared data location
# false = remove downloaded artifacts from the shared data location
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
-->

<!-- ##### Preferences Settings #####

```

```

# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
-->

</agent-input>

```

## Sample response file: Modifying IBM Web Enablement Liberty for IBM i:

You can edit and use this example of a response file for modifying IBM Web Enablement Liberty for IBM i.

```

<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright #####
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2013.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
##### -->

<!-- ##### Frequently Asked Questions #####
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
# Installation Manager Information Center can be found at:
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
# Windows = IBMIM.exe -record c:\temp\responsefiles\WASv85.install.Win32.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
# Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv85.install.RHEL64.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
# Windows = imcl.exe -acceptLicense -showProgress

```

```

# input c:\temp\responsefile\WASv85.install.Win32.xml
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input /home/user/responsefile/WASv85.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
# license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help: IBMIM -help
#
# Question 3. How do I store and pass credentials to repositories that
# require authentication?
# Answer 3. There are two methods for storing authentication credentials
# for Installation Manager depending on the version being used,
# either key ring files or storage files.
#
# Versions of Installation Manager before 1.6.2 use a key ring file to store
# encrypted credentials for authenticating with repositories. Follow this
# two-step process for creating and using a key ring file with Installation Manager.
#
# First, create a key ring file with your credentials by starting
# Installation Manager from the command line under eclipse subdirectory
# with the keyring parameter.
# Use the optional password parameter to password protect your file.
#
# Windows = IBMIM.exe -keyring <path and file name> -password <password>
# Linux, UNIX, IBM i and z/OS = ./IBMIM -keyring <path and file name>
# -password <password>
#
# Installation Manager will start in graphical mode. Verify that the
# repositories to which you need to authenticate are included in the
# preferences, File / Preferences / Repositories. If they are not
# listed, then click Add Repositories to add the URL or UNC path.
# Installation Manager will prompt for your credentials. If the repository
# is already in the list, then any attempt to access the repository location,
# such as clicking the Test Connections button, will also prompt for your
# credentials. Enter the correct credential and check the Save password
# checkbox. The credentials are saved to the key ring file you specified.
#
# Second, when you start a silent installation, run imcl under eclipse/tools
# subdirectory, and provide Installation Manager with the location of the key
# ring file and the password if the file is protected. For example:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <path and file name of response file>
# -keyring <path and name of key ring file> -password <password>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <path and file name of response file>
# -keyring <path and name of key ring file> -password <password>
#
# Versions of Installation Manager at 1.6.2 or higher use storage files
# to store encrypted credentials. Complete the following steps to create
# master password and storage files to use with Installation Manager.
#
# First, if you do not have a master password file already, create a text file
# that contains a master passphrase. An example of a passphrase is:
# "This text is the passphrase for a master password file."
#
# Next, run imutilsc under the eclipse/tools subdirectory with the following
# options to create and store user credentials in a storage file.
# -secureStorageFile <path and file name of storage file>
# -masterPasswordFile <path and file name of master password file>
# -url <repository address> or -passportAdvantage <PPA repository address>
# -userName <user name>
# -userPassword <password for user>
#
# Example of a command to create a storage file by operating system
# Windows = imutilsc saveCredential -url http://myServer -userName myUserName
# -userPassword myPassword -secureStorageFile C:\IBM\credential.store
# -masterPasswordFile C:\IBM\master_password_file.txt
# Linux, UNIX, IBM z/OS, and the OS X operating system =
# ./imutilsc saveCredential -url http://myServer -userName myUserName
# -userPassword myPassword -secureStorageFile /home/IBM/credential.store
# -masterPasswordFile /home/user/IBM/master_password_file.txt
#
# Usage hints:
# * Do not use both the -url and -passportAdvantage options in the same command.
# * Enclose file paths that include spaces with double quotation marks.
# * If you use the IBM service repositories, you can specify the value:
# http://www.ibm.com/software/repositorymanager/entitled/repository.xml
# for the -url option which is a generic service repository for IBM packages.
# * Repeat steps to store credentials for multiple users in one file.
# * Repeat steps to store credentials for multiple repositories in one file.
#
# Afterwards, when you start a silent installation, run imcl under the eclipse/tools
# subdirectory, and provide Installation Manager with the location of the storage
# file. For example:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <path and file name of response file>
# -secureStorageFile <path and name of storage file>

```

```

# -masterPasswordFile <path and name of master password file>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <path and file name of response file>
# -secureStorageFile <path and name of storage file>
# -masterPasswordFile <path and name of master password file>
#
##### -->

<!-- ##### Agent Input #####
#
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the installation finishes.
#
# Valid values for clean:
# true = only use the repositories and other preferences that are
# specified in the response file.
# false = use the repositories and other preferences that are
# specified in the response file and Installation Manager.
#
# Valid values for temporary:
# true = repositories and other preferences specified in the
# response file do not persist in Installation Manager.
# false = repositories and other preferences specified in the
# response file persist in Installation Manager.
#
##### -->

<agent-input clean="true" temporary="true">

<!-- ##### Repositories #####
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#
##### -->

<server>
  <!-- ##### IBM WebSphere Live Update Repositories #####
  # These repositories contain WebSphere Application Server Liberty offerings,
  # and updates for those offerings
  #
  # To use the secure repository (https), you must have an IBM ID,
  # which can be obtained by registering at: http://www.ibm.com/account
  # or your Passport Advantage account.
  #
  # And, you must use a key ring file with your response file.
  ##### -->
  <repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.WEBENAB.v85"/>
  <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

  <!-- ##### Custom Repositories #####
  # Uncomment and update the repository location key below
  # to specify URLs or UNC paths to any intranet repositories
  # and directory paths to local repositories to use.
  ##### -->
  <!-- <repository location="https://w3.mycompany.com/repositories"/> -->
  <!-- <repository location="/home/user/repositories/websphere/" /> -->

  <!-- ##### Local Repositories #####
  # Uncomment and update the following line when using a local
  # repository located on your own machine to install a
  # WebSphere Application Server Liberty offering.
  ##### -->
  <!-- <repository location="insert the full directory path inside single quotes"/> -->
</server>

<!-- ##### Modify Packages #####
#
# Install and Uninstall Commands
#
# Use the install and uninstall commands to inform Installation Manager
# of the installation packages to install or uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
# false = indicates not to modify an existing install by adding
# or removing features.
# true = indicates to modify an existing install by adding or

```

```

#         removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be installed. The offering listed must be present in
# at least one of the repositories listed earlier. The example
# command below contains the offering ID for the WEBENAB
# edition of WebSphere Application Server Liberty.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be installed or uninstalled at the version level
# specified as long as it is available in the repositories. If the version
# attribute is not provided, then the default behavior is to install or
# uninstall the latest version available in the repositories. The version
# number can be found in the repository.xml file in the repositories.
# For example, <offering ... version='8.5.5000.20130328_1111'>.
#
# The profile attribute is required and typically is unique to the
# offering. If modifying or updating an existing installation, the
# profile attribute must match the profile ID of the targeted installation
# of WebSphere Application Server Liberty.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Application Server Liberty include:
# liberty,embeddablecontainer,extprogmodels
#
# The features embeddablecontainer,extprogmodels
# are subfeatures of liberty.
#
# You can use these functions to add or remove feature embeddablecontainer
# or extprogmodels later.
#
# In the example that follows, the feature embeddablecontainer and extprogmodels
# are being added and no feature are being removed from the specified offering.
#
# The installFixes attribute indicates whether fixes available in
# repositories are installed with the product. By default, all
# available fixes will be installed with the offering.
#
# Valid values for installFixes:
#     none = do not install available fixes with the offering.
#     recommended = installs all available recommended fixes with the offering.
#     all = installs all available fixes with the offering.
#
# Installation Manager supports modifying multiple offerings at once.
# Additional offerings can be included in the install and uninstall commands,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to
# WebSphere Application Server Liberty as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, Installing WebSphere Application Server Liberty Offerings on
# a 64-bit system will require to include one of the options for an IBM Software
# Development Kit, this can be specified by data key cic.selector.arch, its value
# can be either x86 (for 32-bit), or x86_64 (for 64-bit).
#
# More details for cic.selector.arch can be found in the link below:
#
# https://infocenters.hursley.ibm.com/was/vNext/draft/help/index.jsp?topic=%2Fcom.ibm.websphere.wlp.core.doc%2Fae%2Fwlp_ins_installation_dist_silent.html
#
##### -->
<install modify="true">
<offering id="com.ibm.websphere.liberty.WEBENAB.v85" profile="WebSphere Liberty V8.5" features="embeddablecontainer,extprogmodels" />
</install>
<profile id="WebSphere Liberty V8.5" installLocation="/QIBM/ProdData/WebSphere/Liberty/V85/Express">
<data key="eclipseLocation" value="/QIBM/ProdData/WebSphere/Liberty/V85/Express" />
<data key="cic.selector.arch" value="x86_64" />
</profile>

<!-- ##### Shared Data Location #####
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an

```

```

# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared' />
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r5/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
#   true = store downloaded artifacts in the shared data location
#   false = remove downloaded artifacts from the shared data location
#
##### -->
<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
-->

<!-- ##### Preferences Settings #####
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45' />
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
<preference name='offering.service.repositories.areUsed' value='true' />
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
<preference name='http.ntlm.auth.kind' value='NTLM' />
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
<preference name='PassportAdvantageIsEnabled' value='false' />
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false' />
-->

</agent-input>

```

## Sample response file: Uninstalling IBM Web Enablement Liberty for IBM i:

You can edit and use this example of a response file for uninstalling IBM Web Enablement Liberty for IBM i.

```

<?xml version="1.0" encoding="UTF-8"?>

<!-- ##### Copyright #####
# Licensed Materials - Property of IBM (c) Copyright IBM Corp. 2013.
# All Rights Reserved. US Government Users Restricted Rights-Use, duplication
# or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

```

```

##### -->

<!-- ##### Frequently Asked Questions #####
# The latest information about using Installation Manager is
# located in the online Information Center. There you can find
# information about the commands and attributes used in
# silent installation response files.
#
# Installation Manager Information Center can be found at:
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
# Question 1. How do I record a response file using Installation Manager?
# Answer 1. Start Installation Manager from the command line under the
# eclipse subdirectory with the record parameter and it will generate a
# response file containing actions it performed, repositories it used, and
# its preferences settings. Optionally use the -skipInstall parameter if
# you do not want the product to be installed to the machine. Specify a
# new agentDataLocation location value when doing a new installation. Do
# not use an existing agentDataLocation for an installation because it might
# damage the installation data and prevent you from modifying, updating,
# rolling back, or uninstalling the installed packages.
#
# Windows: IBMIM -record <responseFile> -skipInstall <agentDataLocation>
# Linux or UNIX: ./IBMIM -record <responseFile> -skipInstall <agentDataLocation>
#
# For example:
# Windows = IBMIM.exe -record c:\temp\responsefiles\WASv85.install.Win32.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
# Linux or UNIX = ./IBMIM -record /home/user/responsefiles/WASv85.install.RHEL64.xml
# -skipInstall c:\temp\skipInstall\WebSphere_Temp_Registry
#
# Question 2. How do I run Installation Manager silently using response file?
# Answer 2. Create a silent installation response file and run the following command
# from the eclipse\tools subdirectory in the directory where you installed
# Installation Manager:
#
# Windows = imcl.exe -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input <response_file_path_and_name> -log <log_file_path_and_name>
#
# For example:
# Windows = imcl.exe -acceptLicense -showProgress
# input c:\temp\responsefile\WASv85.install.Win32.xml
# Linux, UNIX, IBM i and z/OS = ./imcl -acceptLicense -showProgress
# input /home/user/responsefile/WASv85.install.RHEL64.xml
#
# The -acceptLicense command must be included to indicate acceptance of all
# license agreements of all offerings being installed, updated or modified.
# The -showProgress command shows progress when running in silent mode.
# Additional commands can be displayed by requesting help: IBMIM -help
#
##### -->

<!-- ##### Agent Input #####
# The clean and temporary attributes specify the repositories and other
# preferences Installation Manager uses and whether those settings
# should persist after the uninstall finishes.
#
# Valid values for clean:
# true = only use the repositories and other preferences that are
# specified in the response file.
# false = use the repositories and other preferences that are
# specified in the response file and Installation Manager.
#
# Valid values for temporary:
# true = repositories and other preferences specified in the
# response file do not persist in Installation Manager.
# false = repositories and other preferences specified in the
# response file persist in Installation Manager.
#
##### -->

<agent-input clean="true" temporary="true">

<!-- ##### Repositories #####
# Repositories are locations that Installation Manager queries for
# installable packages. Repositories can be local (on the machine
# with Installation Manager) or remote (on a corporate intranet or
# hosted elsewhere on the internet).
#
# If the machine using this response file has access to the internet,
# then include the IBM WebSphere Live Update Repositories in the list
# of repository locations.
#
# If the machine using this response file cannot access the internet,
# then comment out the IBM WebSphere Live Update Repositories and
# specify the URL or UNC path to custom intranet repositories and
# directory paths to local repositories to use.
#

```

```

##### -->

<server>
  <!-- ##### IBM WebSphere Live Update Repositories #####
    # These repositories contain WebSphere Application Server Liberty offerings,
    # and updates for those offerings
    #
    # To use the secure repository (https), you must have an IBM ID,
    # which can be obtained by registering at: http://www.ibm.com/account
    # or your Passport Advantage account.
    #
    # And, you must use a key ring file with your response file.
    ##### -->
  <!--repository location="http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.WEBENAB.v85"/-->
  <!-- <repository location="https://www.ibm.com/software/rational/repositorymanager/repositories/websphere" /> -->

  <!-- ##### Custom Repositories #####
    # Uncomment and update the repository location key below
    # to specify URLs or UNC paths to any intranet repositories
    # and directory paths to local repositories to use.
    ##### -->
  <!-- <repository location='https:\\w3.mycompany.com\\repositories\' /> -->
  <!-- <repository location='/home/user/repositories/websphere/' /> -->

  <!-- ##### Local Repositories #####
    # Uncomment and update the following line when using a local
    # repository located on your own machine to install a
    # WebSphere Application Server Liberty offering.
    ##### -->
  <!-- <repository location='insert the full directory path inside single quotes' /> -->
</server>

<!-- ##### Uninstall Packages #####
#
# Uninstall Command
#
# Use the uninstall command to inform Installation Manager of the
# installation packages to uninstall.
#
# The modify attribute is optional and can be paired with an install
# command to add features or paired with an uninstall command to
# remove commands. If omitted, the default value is set to false.
# false = indicates not to modify an existing install by adding
# or removing features.
# true = indicates to modify an existing install by adding or
# removing features.
#
# The offering ID attribute is required because it specifies the
# offering to be uninstalled. The example command below contains the
# offering ID for WebSphere Application Server Liberty WEBENAB edition.
#
# The version attribute is optional. If a version number is provided,
# then the offering will be uninstalled at the version level specified
# If the version attribute is not provided, then the default behavior is
# to uninstall the latest version. The version number can be found in
# the repository.xml file in the repositories.
# For example, <offering ... version='8.5.5000.20130326_0211'>.
#
# The profile attribute is required and must match the package group
# name for the offering to be uninstalled.
#
# The features attribute is optional. Offerings always have at least
# one feature; a required core feature which is installed regardless
# of whether it is explicitly specified. If other feature names
# are provided, then only those features will be installed.
# Features must be comma delimited without spaces.
#
# The feature values for WebSphere Application Server Liberty include:
# liberty,embeddablecontainer,extprogmodels
#
# The features embeddablecontainer,extprogmodels
# are subfeatures of liberty.
#
# Installation Manager supports uninstalling multiple offerings at once.
# Additional offerings can be included in the uninstall command,
# with each offering requiring its own offering ID, version, profile value,
# and feature values.
#
# Profile Command
#
# A separate profile command must be included for each offering listed
# in the install command. The profile command informs Installation
# Manager about offering specific properties or configuration values.
#
# The installLocation specifies where the offering will be installed.
# If the response file is used to modify or update an existing
# installation, then ensure the installLocation points to the
# location where the offering was installed previously.
#
# The eclipseLocation data key should use the same directory path to

```

```

# WebSphere Application Server Liberty as the installationLocation attribute.
#
# Include data keys for product specific profile properties.
# For instance, Installing WebSphere Application Server Liberty Offerings on
# a 64-bit system will require to include one of the options for an IBM Software
# Development Kit, this can be specified by data key cic.selector.arch, its value
# can be either x86 (for 32-bit), or x86_64 (for 64-bit).
#
# More details for cic.selector.arch can be found in the link below:
#
# https://infocenters.hursley.ibm.com/was/vNext/draft/help/index.jsp?topic=%2Fcom.ibm.websphere.wlp.core.doc%2Fae%2Ftwlp_ins_installation_dist_silent.html
#
##### -->

<uninstall modify="false">
<offering id="com.ibm.websphere.liberty.WEBENAB.v85" profile="WebSphere Liberty V8.5" features="liberty,embeddablecontainer,extprogmodels" />
</uninstall>
<profile id="WebSphere Liberty V8.5" installLocation="/QIBM/ProdData/WebSphere/Liberty/V85/Express">
<data key="eclipseLocation" value="/QIBM/ProdData/WebSphere/Liberty/V85/Express" />
<data key="cic.selector.arch" value="x86_64" />
</profile>

<!-- ##### Shared Data Location #####
# Uncomment the preference for eclipseCache to set the shared data
# location the first time you use Installation Manager to do an
# installation.
#
# Eclipse cache location can be obtained from the installed.xml file found in
# Linux/Unix: /var/ibm/InstallationManager
# Windows: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
# from the following property:
# <property name='cacheLocation' value='C:\Program Files\IBM\IMShared' />
#
# Open the installed.xml file in a text editor because the style sheet
# might hide this value if opened in a web browser.
# For further information on how to edit preferences, refer to the public library at:
# http://publib.boulder.ibm.com/infocenter/install/v1r5/index.jsp?topic=/com.ibm.silentinstall12.doc/topics/r_silent_prefs.html
#
# After the shared data location is set, it cannot be changed
# using a response file or the graphical wizard.
#
# Ensure that the shared data location is a location that can be written
# to by all user accounts that are expected to use Installation Manager.
#
# By default, Installation Manager saves downloaded artifacts to
# the shared data location. This serves two purposes.
#
# First, if the same product is installed a more than once to the machine,
# then the files in the shared data location will be used rather than
# downloading them again.
#
# Second, during the rollback process, the saved artifacts are used.
# Otherwise, if the artifacts are not saved or are removed, then
# Installation Manager must have to access the repositories used to
# install the previous versions.
#
# Valid values for preserveDownloadedArtifacts:
# true = store downloaded artifacts in the shared data location
# false = remove downloaded artifacts from the shared data location
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IMShared' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
-->

<!-- ##### Preferences Settings #####
# Additional preferences for Installation Manager can be specified.
# These preference correspond to those that are located in the graphical
# interface under File / Preferences.
#
# If a preference command is omitted from or commented out of the response
# file, then Installation Manager uses the preference value that was
# previously set or the default value for the preference.
#
# Preference settings might be added or deprecated in new versions of
# Installation Manager. Consult the online Installation Manager
# Information Center for the latest set of preferences and
# descriptions about how to use them.
#
# http://publib.boulder.ibm.com/infocenter/install/v1r6/index.jsp
#
##### -->

<!--
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45' />
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
<preference name='offering.service.repositories.areUsed' value='true' />

```

```

<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
-->

</agent-input>

```

## Installing Liberty on z/OS

### 8.5.5.0

You install the offering by using IBM Installation Manager. Installation Manager installs offerings from one or more product repositories.

### About this task

**Note:** 8.5.5.11 Support for using Java SE 6 with WebSphere Liberty ends in September 2017. After the end of support, the Liberty kernel will be recompiled and can no longer run with Java SE 6. If you continue to use Java SE 6 on earlier fix packs after the end of support date, you could expose your environment to security risks.

Java SE 8 is the recommended Java SDK because it provides the latest features and security updates.

To install WebSphere Application Server Liberty for z/OS, you need both of the following:

- Installation Manager Version 1.5.2 or later running on a z/OS system
  - To create an Installation Manager on z/OS, use one of the following procedures:
    - Install the Installation Manager installation kit (FMID HGIN140) by using SMP/E, and run batch jobs to create the Installation Manager.
    - Download the Installation Manager installation kit as a compressed file, extract it to your z/OS system, and invoke shell commands to create the Installation Manager.

**Tip:** To extract the file, you can use the unzip utility from the z/OS Unix System Services ported tools page.

**Note:** 8.5.5.4 To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

- Access to a copy of the product repository at Fix Pack 8.5.5.0 or later.
  - Perform one of the following procedures:
    - Install the WebSphere Application Server Liberty for z/OS repository (FMID HBBO850) by using SMP/E, and apply the PTFs for Fix Pack 8.5.5.0 or later.
    - Copy the compressed product repositories from the WebSphere Application Server Version 8.5.5 media to your z/OS system, and uncompress them.

### 8.5.5.1

If you are installing WebSphere Application Server Liberty Version 8.5.5.1 in console mode, you might receive warning messages similar to the following example:

```
No "conClass" attribute in "commonPanel" element of panel com.ibm.was.liberty.userdata.panel.UserData in com.ibm.was.liberty.userdata.panel.
```

This problem is caused by an IBM Installation Manager API which is deprecated in Version 1.6.2. These warning messages can be ignored. No action is required.

## Procedure

1. Create an Installation Manager.  
Perform the following procedures:
  - “Obtaining an Installation Manager installation kit for installing Liberty on z/OS”
  - “Creating an Installation Manager for installing Liberty on z/OS” on page 1345
2. Obtain the product repositories.  
Perform the following procedure: “Obtaining repositories for installing Liberty on z/OS” on page 1348.

3.  **8.5.5.6** Optional: Configure an instance of the Liberty Asset Repository Service or a local directory-based repository.  
As part of installing Liberty, you can choose to install assets from the following repositories:
  - The IBM WebSphere Liberty Repository, a public IBM-hosted repository that is accessible through the internet. For more information, see “Liberty: Liberty Repository” on page 965.
  - The Liberty Asset Repository Service, an open-source service that you can use to create an on-premises repository that is remotely accessible behind the firewall of an enterprise. For more information, see the WASdev/tool.lars project on GitHub.
  - Local directory-based repositories that are created by using the **installUtility download** action. For more information, see “Downloading assets using the installUtility command” on page 1400.

Access to the IBM WebSphere Liberty Repository is enabled by default and requires internet access. If your system does not have internet access or you want to install customized Liberty assets, set up an instance of the Liberty Asset Repository Service or a local directory-based repository, and then add the repository in Installation Manager. For more information about the Liberty repositories, see “Installing assets using Installation Manager” on page 1411.

4. Install WebSphere Application Server Liberty for z/OS.  
Perform the following procedure: “Installing WebSphere Application Server Liberty for z/OS” on page 1353.

## What to do next

You can use Installation Manager to install the Web Server Plug-ins for WebSphere Application Server on z/OS, IBM WebSphere SDK Java Technology Edition Version 7.0, and the IBM HTTP Server for WebSphere Application Server for z/OS.

## Obtaining an Installation Manager installation kit for installing Liberty on z/OS

### 8.5.5.0

The installation kit for the IBM Installation Manager is provided with the WebSphere Application Server Liberty for z/OS offering as FMID HGIN140. You can also download the IBM Installation Manager Version 1.5.2 installation kit to your z/OS system.

## Procedure

- To install the IBM Installation Manager installation kit with SMP/E:
  - If you ordered the WebSphere Application Server Liberty for z/OS offering as part of a ServerPac or SystemPac, the IBM Installation Manager installation kit will already be installed. PTFs must be installed to bring the installation kit up to Installation Manager Version 1.5.2, the minimum Installation Manager level for WebSphere Application Server Liberty for z/OS.  
Mount the installation kit file system at a location of your choice.
  - If you ordered the WebSphere Application Server Liberty for z/OS offering as part of a Custom-Built Product Delivery Offering (CBPDO), the IBM Installation Manager installation kit will be included in the CBPDO as FMID HGIN140. Install this offering following the instructions in the

Installation Manager program directory. PTFs must be installed to bring the installation kit up to Installation Manager Version 1.5.2, the minimum Installation Manager level for WebSphere Application Server Liberty for z/OS.

Mount the installation kit file system at a location of your choice.

- To install the IBM Installation Manager installation kit from a downloaded compressed file:
  1. Download a current Installation Manager kit for z/OS from Installation Manager and Packaging Utility download links.
  2. Copy the Installation Manager kit in binary to your z/OS system; for example, using FTP.
  3. Extract the installation files to a directory, such as `/usr/lpp/InstallationManager/V1R4`, using an `unzip` or `jar` command. You can obtain an `unzip` command for z/OS from IBM z/OS Unix System Services Ported Tools. If you use the `jar` command to extract the installation files, you must restore the file permissions and the execute permissions for the extracted files:

```
chmod -R 755 /usr/lpp/InstallationManager/V1R4
```

4. To set extended attributes for the installation files, run the `./set-ext-attr.sh` command. After the command completes, you can remount the installation files as read-only.

## What to do next

When the Installation Manager installation kit is available on your z/OS system, you can use it to create an Installation Manager. See “Creating an Installation Manager for installing Liberty on z/OS.”

## Creating an Installation Manager for installing Liberty on z/OS

**8.5.5.0**

You can create one or more Installation Managers on your z/OS system to install and maintain software products.

### Before you begin

In order to install WebSphere Application Server Liberty for z/OS, your Installation Manager must be at Version 1.5.2 or later.

Install the fix for z/OS APAR OA34228 on each z/OS system that will run IBM Installation Manager to allow the copying of files with extended attributes.

Decide in which of the following modes you want to run the Installation Manager:

#### admin mode

In admin mode, the Installation Manager is installed from a superuser ID (`uid=0`) and can be invoked from any superuser ID. There can only be one admin-mode Installation Manager on a system.

#### user mode

In user mode (also called nonAdmin mode), the Installation Manager can be invoked only by the user that installed it. There can only be one user-mode Installation Manager for a user.

#### group mode

In group mode, the Installation Manager can be invoked by any user ID that is connected to the owning group for the Installation Manager (the default group of the user ID that creates it). There is no limit to the number of group-mode Installation Managers that you can have on a system.

The Installation Manager will consist of two sets of files - a set of executable files that are copied or updated from the installation kit, and a set of runtime data files that describe the products installed by this Installation Manager. Both sets of files must be writeable by the Installation Manager. You must select locations for both the executable and runtime data for each Installation Manager.

Table 93. Default locations for Installation Manager files. The following table shows the default locations for the Installation Manager executable files (binaries) and runtime data on z/OS.

Files	Admin or group mode	User mode
Binaries	/InstallationManager/bin	\$HOME/InstallationManager/bin
Runtime data (also called agent data)	/InstallationManager/appdata	\$HOME/InstallationManager/appdata

These locations are assumed in the Installation Manager documentation and sample jobs. If these names are not appropriate for your system or if you choose to have several Installation Managers, you can choose different names and specify them when you create the Installation Manager.

## Procedure

1. Make sure that the fix for z/OS APAR OA34228 is installed on your z/OS system.
2. Create a user ID and group to own the Installation Manager.

This user ID must have the following attributes:

- Read/write home directory
- Read access to FACILITY profile BPX.FILEATTR.APF
- Read access to FACILITY profile BPX.FILEATTR.PROGCTL
- Read access to FACILITY profile BPX.FILEATTR.SHARELIB
- Read access to UNIXPRIV profile SUPERUSER.FILESYS.CHOWN
- Read access to UNIXPRIV profile SUPERUSER.FILESYS.CHANGEPERMS

The user ID that creates the Installation Manager will become the initial (possibly only) user ID that can invoke that particular Installation Manager. If you create an Installation Manager in group mode, the default group for this user will become the owning group for the Installation Manager. This user ID must have a read/write home directory.

You can use an existing user ID if it meets these requirements.

If you installed the Installation Manager installation kit with SMP/E, you can use the Installation Manager sample job GIN2ADMN in SGINJCL to create this user ID and group as well as to assign appropriate permissions.

When you invoke a group mode Installation Manager, your effective group must be the same as the group that created the Installation Manager.

It is no longer necessary to set your umask to allow group-write when invoking a group-mode Installation Manager. Instead, an Installation Manager running in group mode will turn on group-write by default then reset the umask to its previous value when Installation Manager processing is complete.

3. If the Installation Manager binaries and runtime data will not reside in existing read/write file systems, create file systems for the data and mount the file systems read/write.

The file systems should be owned by the user ID and group that will create the Installation Manager and have permissions 755 for an admin or user-mode Installation Manager or 775 for a group-mode Installation Manager.

If you installed the Installation Manager installation kit with SMP/E, you can use the Installation Manager sample job GIN2CFS in SGINJCL to allocate and mount a file system to hold the binaries and runtime data.

The Installation Manager creation process described in this topic will create the binaries and runtime data directories if they do not already exist.

4. Log in to the Unix system services shell under the owning user ID for the Installation Manager, and change the directory to the location of the Installation Manager installation kit.

```
cd /usr/lpp/InstallationManager/V1R5
```

The installation kit must be at Version 1.5.2 or later.

5. Run the **installc**, **userinstc**, or **groupinstc** command from the installation kit to create the Installation Manager.

- To create an Installation Manager in admin mode, issue the following command from the shell:

```
installc -acceptLicense  
-installationDirectory binaries_location  
-dataLocation appdata_location
```

- To create an Installation Manager in user mode, issue the following command from the shell:

```
userinstc -acceptLicense  
-installationDirectory binaries_location  
-dataLocation appdata_location
```

- To create an Installation Manager in group mode, issue the following command from the shell:

```
groupinstc -acceptLicense  
-installationDirectory binaries_location  
-dataLocation appdata_location
```

You can omit the **-installationDirectory** and **-dataLocation** parameters if you use the default locations.

If you used SMP/E to install the Installation Manager installation kit, you can use sample job GIN2INST in SGINJCL to create an Installation Manager.

6. You can now unmount the Installation Manager installation kit.

## What to do next

You can verify that the Installation Manager is correctly installed by logging in to the Unix System Services shell under the user ID that created the Installation Manager and running the Installation Manager `imcl` command from the `eclipse/tools` subdirectory of the Installation Manager's binaries location. For example:

```
cd /InstallationManager/bin/eclipse/tools  
imcl -version
```

You are now ready to install products using IBM Installation Manager.

**Authorizing additional users to a group-mode Installation Manager:** To allow additional users to access a group-mode Installation Manager, make sure that they meet the requirements listed in the first step of the procedure described previously and then connect them to the owning group for the Installation Manager using the TSO CONNECT command:

```
CONNECT user2 GROUP(IMGROUP)
```

To create an additional Installation Manager, follow the steps in the procedure described previously, selecting a new user ID and group (if appropriate) and new binaries and runtime data locations. Do not share binaries or runtime data locations between separate Installation Managers.

**Correcting file ownership or permission problems:** If you accidentally invoke an Installation Manager from the wrong user ID, some files might end up with ownerships that prevent normal use of the Installation Manager. To correct this problem, log on to a super user or other privileged user ID and reset the file ownership and permissions for the Installation Manager binaries and runtime data. For example:

```
chown IMADMIN:IMGROUP /InstallationManager/bin  
chmod 775 /InstallationManager/bin  
  
chown IMADMIN:IMGROUP /InstallationManager/appdata  
chmod 775 /InstallationManager/appdata
```

If the users of a group-mode Installation Manager do not have `umask` set to allow group-write permission on created files, you might also have to perform this step when switching from one user ID to another. You might also need to set permissions and owners for the product files that you install with the Installation Manager to ensure that maintenance can be performed from other user IDs in the group.

**Upgrading the Installation Manager:** To upgrade an Installation Manager to a new level of the Installation Manager product, download or install the new level of the IBM Installation Manager

installation kit and mount it on your system. Then, change directory to the new level of the installation kit and reissue the same **installc**, **userinstc**, or **groupinstc** command that you used to create the Installation Manager. This will update the Installation Manager's binaries from the new installation kit.

## Obtaining repositories for installing Liberty on z/OS

8.5.5.0

WebSphere Application Server Liberty for z/OS offerings are distributed as IBM Installation Manager repositories. These repositories contain the metadata and files that are required to create one or more levels of a particular product.

### About this task

The initial repository for the WebSphere Application Server Liberty for z/OS offering can be obtained by one of the following methods:

- Installing with SMP/E by using a ServerPac, SystemPac, or Customer-Build Product Delivery Offering (CBPDO)

This results in a repository file system that contains the initial repositories for WebSphere Application Server for z/OS (including the WebSphere Application Liberty Server Liberty for z/OS offering), IBM HTTP Server for z/OS, and Web Server Plug-ins for WebSphere Application Server for z/OS. An optional second repository contains the code for IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty.

- Copying the initial (compressed) product repositories from the product physical media or ShopzSeries to your z/OS system, and uncompressing them

When you place an order for the product (CBPDO or ServerPac) on ShopzSeries, you can select whether you want to receive either a physical tape delivery or an internet/electronic delivery.

- If you select physical tape delivery, you receive a CD or DVD that includes the IBM WebSphere Application Server Liberty for z/OS compressed repositories in a compressed file in the Additional Material directory of the CD or DVD.
- If you select internet/electronic delivery, the WebSphere Application Server Liberty for z/OS compressed repositories are shipped to you as an ISO file. You can then burn the ISO file to a CD or DVD, or you can use virtualcd software to mount and process the ISO file on your workstation.

New service levels can be installed from the web-based service repositories or downloaded as service repositories that contain extra product code. Each service repository contains all the necessary materials to upgrade any previous service level of WebSphere Application Server Liberty for z/OS to the level of the service repository.

- Applying PTFs to an SMP/E-based repository adds a single level of the service repository for each component to the SMP/E-managed repository.
- Downloading service repositories from Fix Central allows you to upgrade WebSphere Application Server components to new service levels.

Perform this procedure to obtain the repositories for WebSphere Application Server Liberty for z/OS.

### Procedure

- To install initial repositories by using SMP/E, perform the following procedure.
  1. Order an IBM ServerPac, SystemPac, or CBPDO for the WebSphere Application Server Liberty for z/OS offering.

It contains the following FMIDs:

#### HBBO850

Product repository for WebSphere Application Server for z/OS (including the WebSphere

Application Liberty Server Liberty for z/OS offering), IBM HTTP Server for z/OS, and Web Server Plug-ins for WebSphere Application Server for z/OS

### **HBJA700**

Product repository for IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty

This FMID is only needed if you plan to use IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty with WebSphere Application Server Liberty for z/OS Version 8.5.5.

2. Verify that the PTFs for Fix Pack 8.5.5.0 or later, are available and are installed.
3. Install the product repositories according to the instructions in your order.

Mount the base repository (FMID HBBO850) at a location of your choice. In the examples in this documentation, this repository is mounted at:

```
/usr/lpp/InstallationManagerRepository/HBBO850
```

If you plan to use IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty with WebSphere Application Server Liberty for z/OS Version 8.5.5, mount the repository at a location of your choice. In the examples in this documentation, these repositories are mounted at:

```
/usr/lpp/InstallationManagerRepository/HBJA700
```

- To install initial repositories without SMP/E, perform the following procedure.
  1. Obtain product media at Fix Pack 8.5.5.0 or later.
  2. Copy the following files from the media to your z/OS system. If you use FTP, be sure to transfer the files in binary format.

#### **was.repo.8550.liberty.zOS.zip**

Initial repository for WebSphere Application Server Liberty for z/OS

#### **was.repo.8550.plg.zip**

Initial repository for Web Server Plug-ins for WebSphere Application Server for z/OS

#### **was.repo.8550.ihs.zip**

Initial repository for IBM HTTP Server for z/OS

3. If you plan to use IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty with WebSphere Application Server Liberty for z/OS Version 8.5.5, copy the following file from the product media to your z/OS system. If you use FTP, be sure to transfer the file in binary format.

#### **was.repo.8550.java7.zip**

Initial repository for IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty

Uncompress each file into an empty directory. You can download an extract utility from z/OS Unix System Services ported tools.

## **Results**

If you installed the initial repository with SMP/E, you now have a single repository file system that contains materials for WebSphere Application Server Liberty for z/OS, IBM HTTP Server for z/OS, and Web Server Plug-ins for WebSphere Application Server for z/OS and a second (optional) file system that contains the IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty repository. Each repository file system contains the initial product level. If PTFs are installed, each repository file system contains a single product service level.

If you installed the initial repositories without SMP/E, you now have separate directories that contain the initial product repositories for WebSphere Application Server Liberty for z/OS, IBM HTTP Server for z/OS, Web Server Plug-ins for WebSphere Application Server for z/OS, and IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty (optional).

These repositories can be supplemented with materials from the web-based service repository or from downloaded service repositories. Service repositories can be obtained from Fix Central.

These repositories contain the necessary files to install the product code for WebSphere Application Server Liberty for z/OS, including IBM HTTP Server for z/OS, Web Server Plug-ins for WebSphere Application Server for z/OS, and IBM WebSphere SDK Java Technology Edition Version 7.0 for Liberty.

## What to do next

When you use IBM Installation Manager to install WebSphere Application Server Liberty for z/OS, specify the path to the appropriate repository in the **-repositories** parameter of the **imcl** command.

## Creating custom installation repositories with IBM Packaging Utility

8.5.5.0

IBM WebSphere Application Server Liberty uses IBM Installation Manager for installation and lifecycle management. Installation Manager accesses source repositories that contain the content for a software product installation. Repositories are available on product media, in IBM-hosted web-based repositories, and from Passport Advantage. IBM Packaging Utility can help you create and customize enterprise repositories that contain the correct combination of products and maintenance levels needed for all aspects of your business.

### About this task

You use Installation Manager to connect to an Installation Manager repository (or set of repositories) to find products and service updates that are available to you for installation. An Installation Manager repository is simply a tree-structured file folder that includes product payload and metadata. You can install the software products that you need directly from an IBM web-based service repository or download and unpack compressed files from Passport Advantage and install the products from the resulting unpacked file folders. The result of unpacking the files is also considered to be an Installation Manager repository. Like any Installation Manager repository, these unpacked files can be hosted on an internal HTTP server, FTP server, or network mount in order to make them available to the organization.

Packaging Utility is a companion tool for Installation Manager with which you can create and manage custom Installation Manager repositories for your organization. You can copy multiple packages, maintenance levels, and fixes into a single repository. Packaging Utility copies from source repositories to your target custom repositories. Source repositories can include any accessible Installation Manager repository, including IBM web-hosted product repositories and unzipped Passport Advantage downloads.

For more information on Packaging Utility, go to the IBM Packaging Utility Information Center.

### Procedure

Use Packaging Utility to create custom or "enterprise" Installation Manager repositories that contain specific products and maintenance levels that fit the needs of your business.

As an administrator, you can control the content of your enterprise repository, which then can serve as the central repository to which your organization connects in order to perform product installations and updates.

Packaging Utility essentially copies from a set of source Installation Manager repositories to a target repository and eliminates duplicate artifacts, helping to keep the repository size as small as possible. You can also delete (or "prune") a repository, removing maintenance levels or products that are not needed. You can download the latest version of Packaging Utility from the IBM Support Portal.

Like Installation Manager, Packaging Utility has GUI and command-line interfaces. You must specify repository URLs for Installation Manager repositories that contain the offerings that you wish to copy. Installation Manager repository URLs follow this pattern:

[http://www.ibm.com/software/repositorymanager/offering\\_name](http://www.ibm.com/software/repositorymanager/offering_name)

**Note:** This location does not contain a web page that you can access using a web browser. For example, WebSphere Application Server Liberty product repositories are located at the following URLs:

- WebSphere Application Server Liberty Network Deployment Version 8.5  
`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85`
- WebSphere Application Server Liberty Network Deployment Trial Version 8.5  
`http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.NDTRIAL.v85`

See Online product repositories for WebSphere Application Server offerings for additional product repositories.

The target repository that you create with Packaging Utility will always support a full installation; therefore, you cannot use Packaging Utility to create a repository that is only a copy of a fix pack. You can, however, create a repository that contains the minimum content to support direct installation to a fix-pack level. Consider the following two examples that use the Packaging Utility command-line interface (**PUCL.exe**) that is available in the Packaging Utility installation folder.

- **Example 1**

**Note:** Note that you must read the license agreement that you can find with the product files and then signify your acceptance of the license agreement by specifying **-acceptLicense** in the command as shown in the following example.

```
PUCL copy com.ibm.websphere.liberty.ND.v85
-repositories
  http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85
-target D:\LIB_ND_version
-prompt
-showProgress
-acceptLicense
```

Since no version number is specified with the offering name, this command will create a new repository that supports direct installation to the latest fix-pack level for WebSphere Application Server Liberty Version 8.5. This new repository does not support the installation of Version 8.5.5.0, but it does support the update from an existing Version 8.5.5.0 installation to the latest version.

- **Example 2**

```
PUCL copy com.ibm.websphere.liberty.ND.v85_8.5.5.0.20110503_0200
-repositories
  http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85
-target D:\LIB_ND
-prompt
-showProgress
-acceptLicense
```

```
PUCL copy com.ibm.websphere.liberty.ND.v85_8.5.5.1.20110829_1838
-repositories
  http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.ND.v85
-target D:\LIB_ND
-prompt
-showProgress
-acceptLicense
```

The first command creates a target repository with WebSphere Application Server Liberty Version 8.5.5.0. The second command adds the Version 8.5.5.1 fix pack to the same repository. You can now use this resulting repository to install Version 8.5.5.0, install Version 8.5.5.1, or update from Version 8.5.5.0 to Version 8.5.5.1.

**Tip:** With some offerings, such as WebSphere SDK Java Technology Edition Version 7.0 for Liberty, you can use Packaging Utility with the **-platform** option (sometimes called "platform slicing") to create a repository that is scoped to the platforms and architectures that are used by your organization. This feature is available in command-line mode by specifying the **-platform** option with the `os` and `arch` arguments as shown in the following example:

```

PUCL copy com.ibm.websphere.liberty.IBMJAVA.v70
-repositories http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v70
-platform os=linux,arch=ppc64
-target D:\LIB_ND
-prompt
-showProgress
-acceptLicense</p>

```

Your repository can be scoped for platforms other than the one on which it is created or stored. For example, you can run Packaging Utility on a Windows system to create a repository with the content needed to install on a Linux system. During installation on Linux, you point Installation Manager to your custom repository.

The following table lists valid combinations for creating a local WebSphere SDK Java Technology Edition Version 7.0 for Liberty offering repository that is sliced by operating system and architecture.

*Table 94. Valid combinations for creating a local WebSphere SDK Java Technology Edition Version 7.0 for Liberty offering repository using the Packaging Utility*

Platform	Options	Resulting Repository
Windows	os=win32,arch=x86	32-bit repository for 32-bit Windows OS and 64-bit Windows
	os=win32.arch=x86_64	64-bit repository for 64-bit Windows
Linux Intel	os=linux,arch=x86	32-bit repository for 32-bit Linux Intel and 64-bit Linux Intel
	os=linux.arch=x86_64	64-bit repository for 64-bit Linux Intel
Linux Power	os=linux,arch=ppc	32-bit repository for 32-bit Linux Power and 64-bit Linux Power
	os=linux.arch=ppc64	64-bit repository for 64-bit Linux Power
zLinux	os=linux,arch=s390	32-bit repository for 32-bit zLinux and 64-bit zLinux
	os=linux.arch=s390x	64-bit repository for 64-bit zLinux
AIX	os=aix,arch=ppc	32-bit repository for 32-bit AIX and 64-bit AIX
	os=aix.arch=ppc64	64-bit repository for 64-bit AIX
Solaris Sparc	os=solaris,arch=sparc	32-bit repository for 32-bit Solaris Sparc and 64-bit Solaris Sparc
	os=solaris,arch=sparc64	64-bit repository for 64-bit Solaris Sparc
Solaris Intel	os=solaris,arch=x86_64	64-bit repository for 64-bit Solaris Intel
HP-UX Itanium	os=hpux,arch=ia64	64-bit repository for 64-bit HP-UX Itanium
z/OS	os=zos,arch=s390x	64-bit repository for z/OS

The following table lists valid combinations for creating a local WebSphere SDK Java Technology Edition Version 6.0 for Liberty offering repository that is sliced by operating system and architecture.

Table 95. Valid combinations for creating a local WebSphere SDK Java Technology Edition Version 6.0 for Liberty offering repository using the Packaging Utility

Platform	Options	Resulting Repository
Windows	os=win32,arch=x86	32-bit repository for 32-bit Windows OS and 64-bit Windows
	os=win32.arch=x86_64	64-bit repository for 64-bit Windows
Linux Intel	os=linux,arch=x86	32-bit repository for 32-bit Linux Intel and 64-bit Linux Intel
	os=linux.arch=x86_64	64-bit repository for 64-bit Linux Intel
Linux Power	os=linux,arch=ppc	32-bit repository for 32-bit Linux Power and 64-bit Linux Power
	os=linux.arch=ppc64	64-bit repository for 64-bit Linux Power
zLinux	os=linux,arch=s390	32-bit repository for 32-bit zLinux and 64-bit zLinux
	os=linux.arch=s390x	64-bit repository for 64-bit zLinux
AIX	os=aix,arch=ppc	32-bit repository for 32-bit AIX and 64-bit AIX
	os=aix.arch=ppc64	64-bit repository for 64-bit AIX
Solaris Sparc	os=solaris,arch=sparc	32-bit repository for 32-bit Solaris Sparc and 64-bit Solaris Sparc
	os=solaris,arch=sparc64	64-bit repository for 64-bit Solaris Sparc
Solaris Intel	os=solaris,arch=x86_64	64-bit repository for 64-bit Solaris Intel
HP-UX Itanium	os=hpx,arch=ia64	64-bit repository for 64-bit HP-UX Itanium

For more information on platform slicing, go to the IBM Packaging Utility Information Center.

## Installing WebSphere Application Server Liberty for z/OS

### 8.5.5.0

The product code for WebSphere Application Server Liberty for z/OS is installed using IBM Installation Manager.

### Before you begin

Create an Installation Manager on your z/OS system. You will need to know the location of the binaries directory for the Installation Manager and have access to a user ID that can invoke the Installation Manager.

Obtain the product repository for WebSphere Application Server Liberty for z/OS. The repository can be mounted read-only.



### 8.5.5.2

To install assets from the IBM WebSphere Liberty Repository, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later.



### 8.5.5.6

If you want to install Liberty assets from local directory-based repositories or an instance of the Liberty Asset Repository Service, configure the repositories. For more information about the Liberty

asset repositories, see “Installing assets using Installation Manager” on page 1411.

## About this task

**8.5.5.4** To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

## Procedure

1. Choose an installation location for this copy of WebSphere Application Server Liberty for z/OS.

This copy of the product must be mounted at this location every time Installation Manager accesses it to install, uninstall, or modify it. This does not have to be the same location at which the product will be mounted when used in production.

Installation Manager requires that every installed product or group of products have its own installation location.

2. Mount an empty file system read/write at this location.

It will require a minimum of:

- 72 megabytes (2000 tracks (3390)) for WebSphere Application Server Liberty for z/OS with no optional features
- 132 megabytes (4000 tracks (390)) for WebSphere Application Server Liberty for z/OS with all optional features
- 426 megabytes (9000 tracks (3390)) for WebSphere Application Server Liberty for z/OS with all optional features and WebSphere SDK Java Technology Edition Version 7.0 for Liberty

Set the ownership for the file system to that of the Installation Manager user ID, and set the permissions to allow group-write if it will be access by a group-mode Installation Manager. For example:

```
chown IMADMIN:IMGROUP /usr/lpp/zWebSphere/V8R5
```

```
chmod 775 /usr/lpp/zWebSphere/V8R5
```

You can use the `zCreateFileSystem.sh` script in the `eclipse/tools` subdirectory of the Installation Manager binaries location to create this file system. For example:

```
cd /InstallationManager/bin/eclipse/tools
```

```
zCreateFileSystem.sh -name WAS.v85.SBBOHFS -type ZFS  
-megabytes 1800 200 -volume PRV005  
-mountpoint /usr/lpp/zWebSphere/V8R5  
-owner IMADMIN -group IMGROUP
```

If you installed the initial product repository with SMP/E, you can use sample job BBO1CFS in the SBBOJCL dataset to allocate and mount this file system.

3. Log in to the Unix System Services shell under the Installation Manager user ID, and change the directory to the `eclipse/tools` subdirectory of the Installation Manager binaries location.

For example:

```
cd /InstallationManager/bin/eclipse/tools
```

4. If you plan to use the web-based service repository, create a keyring file on z/OS to access this repository by running the `imutilsc` command.

```
installation_manager_binaries_directory/eclipse/tools/imutilsc saveCredential  
-keyring keyring_file  
-userName user_ID -userPassword user_password  
-url http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.zOS.v85/repository.xml
```

where *keyring\_file* is the path and file name of the keyring to be created, and *user\_ID* and *user\_password* are the universal IBM user ID and password that you use to access protected IBM software websites.

For example:

```

/InstallationManager/eclipse/tools/imutilsc saveCredential
-keyring /u/jane/IBM.software.keyring
-userName jsmith01 -userPassword 732Uke1ele
-url http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.z0S.v85/repository.xml

```

Make sure that the keyring file is readable by the Installation Manager user ID.

**Note:** Starting in Installation Manager Version 1.6.2, the **-keyring** and **-password** options that have been used to access credentials in a keyring file are deprecated. When you use Installation Manager Version 1.6.2 and later, use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential storage file. There is no migration path from keyring files to storage files because of the differences in the file structures. You must create a storage file to replace a keyring file. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

5. Verify that the product repositories are available.

You do this by issuing the following Installation Manager command-line command.

```
imcl listAvailablePackages -repositories list_of_repository_locations
```

You should see one or more levels of the WebSphere Application Server Liberty for z/OS offering, `com.ibm.websphere.liberty.z0S.v85`.

The `list_of_repository_locations` should include the path to the initial product repository and the paths to any additional service repositories. Separate URLs in the `list_of_repository_locations` with commas.

To use the web-based service repository, add the **-useServiceRepository** parameter and use the **-keyring** parameter to specify a keyring file containing your IBM Software ID and password. For example:

```

imcl listAvailablePackages
-repositories /usr/lpp/InstallationManagerRepository/HBB0850
-useServiceRepository
-keyring /u/jane/IBM.software.keyring

```

6. Read the product license, which can be found in the `lafiles` subdirectory of the product repository.
7. Run the Installation Manager command-line tool to install the WebSphere Application Server Liberty for z/OS product.

```

imcl install com.ibm.websphere.liberty.z0S.v85
-installationDirectory installation_location
-repositories list_of_repository_locations
-sharedResourcesDirectory shared_data_location
-acceptLicense
[-useServiceRepository -keyring keyring_file]
[-installFixes <all | recommended | none> ]

```

The **-sharedResourcesDirectory** parameter points to a directory in which Installation Manager will store artifacts from the repository during installation processing. This value is set the first time a product is installed with a particular Installation Manager. This directory should have at least 30,000 tracks of free space. You can omit this parameter after the shared resources directory has been set.

By specifying **-acceptLicense**, you accept the terms of the product license. The relevant terms and conditions, notices, and other information are provided in the license-agreement files in the `lafiles` or `product_name/lafiles` subdirectory of the installation image or repository for this offering.

If you do not specify the product version to be installed, Installation Manager will install the latest version of the product along with any fixes in the repository locations. You can prevent the installation of fixes by specifying `-installFixes none` or install only recommended fixes by specifying `-installFixes recommended`.

If you specify the product version to be installed, any fixes in the repository locations will only be installed if you specify `-installFixes recommended` or `-installFixes all`.

You can also follow the package name (and version) with a comma and a list of optional features separated by commas. The following features are available for WebSphere Application Server Liberty for z/OS. The keyword name for each feature is provided in parentheses.

- Embeddable EJB container and JPA client (`embeddablecontainer`)

This option installs the embeddable EJB container and JPA client.

The embeddable EJB container is a Java Archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition (SE) environment. You can run enterprise beans using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.

The JPA client can be used with the embeddable EJB container to provide Java Persistence API capability in a Java SE environment.

- Extended Programming Models - `extprogmodels` (Version 8.5.5.3 and previous)

The Extended Programming Models feature provides a rich set of programming models such as Web Services, JMS (including Message-Driven Beans), and Mongo 2.0.

 **8.5.5.4** As of Fix Pack 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` add-on, or install the individual features that you need. See the complete list of Liberty features.

#### Notes:

- When you install a new copy of the WebSphere Application Server Liberty for z/OS and do not specify the features to be installed, the following features are installed by default:
  - `embeddablecontainer`
  - `extprogmodels` (for fix pack 8.5.5.3 and previous versions)
- If any features are listed, the normal list of default features is ignored and only the listed features are installed.

-  **8.5.5.4** Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` add-on, or install the individual features that you need from the Liberty Repository. See the following topics for more information:

- Installing Liberty Repository assets
- Liberty features

-  **8.5.5.2** You can specify additional assets to install from the Liberty Repository. For a list of Liberty Repository assets, see the downloads page on WASdev.net.

If you want to install Liberty Repository features, specify the short names or symbolic names on the `user.feature` option of the `-properties` parameter. Multiple feature names are separated with double commas. The following example installs the Portlet Container and Portlet Serving features:

```
-properties user.feature=portlet-2.0,,portletserving-2.0,user.accept.license=true
```

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.

In Version 8.5.5.2, you cannot install the `zosLocalAdapters-1.0` or `zosConnect-1.0` features by using Installation Manager. You must use the `featureManager` command to install these features. For more information, see

- “Enabling the Liberty server environment to use optimized local adapters” on page 1697
- “Setting up z/OS Connect” on page 1536

You can install the complete set of Extended Programming Model features by specifying the `user.addon` option:

```
-properties user.addon=extendedPackage-1.0,user.accept.license=true
```

If you upgrade WebSphere Application Server Liberty Version 8.5.5.3 or previous versions that contain the `extprogmodels` feature, Installation Manager automatically installs the `extendedPackage-1.0` add-on. You must specify the `user.accept.license` option:

```
-properties user.accept.license=true
```

**8.5.5.6** You can also install assets from instances of the Liberty Asset Repository Service or local directory-based repositories. For more information about these asset repositories, see “Installing assets using Installation Manager” on page 1411. Add the repository on the `-repositories` parameter. The repositories are accessed in the order that they are specified. By default, the Liberty

Repository is the last of the repositories that are accessed during installation. To disable access to the Liberty Repository, on the **-properties** parameter, set the **user.useLibertyRepository** option to **false**.

8.5.5.8

```
imcl install com.ibm.websphere.liberty.z05.v85
-properties user.useLibertyRepository=false,user.addon=extendedPackage-1.0,user.feature=portlet-2.0
-installationDirectory /usr/lpp/zWebSphere/Liberty/V8558 -acceptLicense
-repositories /usr/lpp/InstallationManagerRepository/HBB0850,
https://your_onprem_asset_repo_url,/WAS855/LocalAssetRepo,/WAS855/LocalAssetRepo2.zip
-sharedResourcesDirectory /InstallationManager/sharedResources
-showProgress
```

To learn more about the Liberty Repository and the assets it contains, see “Liberty: Liberty Repository” on page 965.

If you installed the initial product repository with SMP/E, you can use sample job BBO1INST in the SBBOJCL dataset to perform the product installation.

8. Product installation is complete when the Installation Manager completes without error messages. Logs for the installation can be found in the logs subdirectory of the Installation Manager runtime data location.
9. When product installation is complete, unmount the product filesystem and remount it read-only for use by Liberty servers.

## Installing IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty

8.5.5.0

You can install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty using IBM Installation Manager Version 1.5.2 or later.

### Before you begin

1. Create an Installation Manager on your z/OS system.  
You will need to know the location of the binaries directory for the Installation Manager and have access to a user ID that can invoke the Installation Manager.
2. Install a copy of WebSphere Application Server Liberty for z/OS Version 8.5.
3. Obtain the product repository for IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1. The repository can be mounted read-only.

The repository for IBM WebSphere SDK Java Technology Edition Version 7.0 is part of the WebSphere Application Server for z/OS Version 8.5 product. You can install the repository with SMP/E, download the installation files from the IBM Fix Central, or install the Java SDK directly from the service repository.

8.5.5.2

For WebSphere Application Server for z/OS Version 8.5.5.2 and later, you can also install IBM WebSphere SDK Java Technology Edition Version 7.1. You can download the installation files from the IBM Fix Central, or you can install the Java SDK directly from the service repository. The Java SDK is not available in SMP/E format.

For more information about obtaining product repositories, see “Obtaining repositories for installing Liberty on z/OS” on page 1348.

### Procedure

1. Choose the installed copy of WebSphere Application Server Liberty for z/OS Version 8.5 onto which you will install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty.
2. Mount the product file system for this copy of WebSphere Application Server Liberty for z/OS Version 8.5 at the same location at which it was originally installed with IBM Installation Manager.  
The file system will require a minimum of 7,500 tracks (3390) or 350 megabytes of available disk space to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty.

You can use the `zMountFileSystem.sh` script in the `eclipse/tools` subdirectory of the Installation Manager binaries location to mount this file system. For example:

```
cd /InstallationManager/bin/eclipse/tools
zMountFileSystem.sh -name WAS.V85.SBBOHFS -type ZFS
-mountpoint /usr/lpp/zWebSphere/V8R5
```

You can add the **-owner**, **-group**, and **-perm** options to this command to set the ownership and permissions for all files in the file system.

3. Log in to the Unix System Services shell under the Installation Manager user ID, and change the directory to the `eclipse/tools` subdirectory of the Installation Manager binaries location.

For example:

```
cd /InstallationManager/bin/eclipse/tools
```

4. If you plan to use the web-based service repository, create a keyring file on z/OS to access this repository by running the **imutilsc** command, where *keyring\_file* is the path and file name of the keyring to be created, and *user\_ID* and *user\_password* are the universal IBM user ID and password that you use to access protected IBM software websites.

IBM WebSphere SDK Java Technology Edition Version 7.0:

```
installation_manager_binaries_directory/eclipse/tools/imutilsc saveCredential
-keyring keyring_file
-userName user_ID -userPassword user_password
-url http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v70/repository.xml
```

**8.5.5.2**

IBM WebSphere SDK Java Technology Edition Version 7.1:

```
installation_manager_binaries_directory/eclipse/tools/imutilsc saveCredential
-keyring keyring_file
-userName user_ID -userPassword user_password
-url http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v71/repository.xml
```

The following example creates a keyring file for IBM WebSphere SDK Java Technology Edition Version 7.0:

```
/opt/IBM/InstallationManager/eclipse/tools/imutilsc saveCredential
-keyring /u/jane/IBM.software.keyring
-userName jsmith01 -userPassword 732Ukelele
-url http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v70/repository.xml
```

**8.5.5.2**

The following example creates a keyring file for IBM WebSphere SDK Java Technology Edition Version 7.1:

```
/opt/IBM/InstallationManager/eclipse/tools/imutilsc saveCredential
-keyring /u/jane/IBM.software.keyring
-userName jsmith01 -userPassword 732Ukelele
-url http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v71/repository.xml
```

Make sure that the keyring file is readable by the Installation Manager user ID.

**Note:** Starting in Installation Manager Version 1.6.2, the **-keyring** and **-password** options that have been used to access credentials in a keyring file are deprecated. When you use Installation Manager Version 1.6.2 and later, use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential storage file. There is no migration path from keyring files to storage files because of the differences in the file structures. You must create a storage file to replace a keyring file. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

5. Verify that the product repository is available.

You do this by issuing the following Installation Manager command-line command.

```
imcl listAvailablePackages -repositories list_of_repository_locations
```

You should see one or more levels of the IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty offering:

- **8.5.5.0** com.ibm.websphere.liberty.IBMJAVA.v70
- **8.5.5.2** com.ibm.websphere.liberty.IBMJAVA.v71

The *list\_of\_repository\_locations* should include the path to the initial product repository and the paths to any additional service repositories. Separate URLs in the *list\_of\_repository\_locations* with commas. To use the web-based service repository, add the **-useServiceRepository** parameter and use the **-keyring** parameter to specify a keyring file containing your IBM Software ID and password. For example:

```
imcl listAvailablePackages
-repositories /usr/lpp/InstallationManagerRepository/HBB0850
-useServiceRepository
-keyring /u/jane/IBM.software.keyring
```

**Note:** Starting in Installation Manager Version 1.6.2, the **-keyring** and **-password** options that have been used to access credentials in a keyring file are deprecated. When you use Installation Manager Version 1.6.2 and later, use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential storage file. There is no migration path from keyring files to storage files because of the differences in the file structures. You must create a storage file to replace a keyring file. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

6. Run the Installation Manager command-line tool to install IBM WebSphere SDK Java Technology Edition Version 7.0 or 7.1 for Liberty.

IBM WebSphere SDK Java Technology Edition Version 7.0:

```
imcl install com.ibm.websphere.liberty.IBMJAVA.v70
-installationDirectory installation_location
-repositories list_of_repository_locations
-sharedResourcesDirectory shared_data_location
-acceptLicense
[-useServiceRepository -keyring keyring_file]
[-installFixes <all | recommended | none> ]
```

### 8.5.5.2

IBM WebSphere SDK Java Technology Edition Version 7.1:

```
imcl install com.ibm.websphere.liberty.IBMJAVA.v71
-installationDirectory installation_location
-repositories list_of_repository_locations
-sharedResourcesDirectory shared_data_location
-acceptLicense
[-useServiceRepository -keyring keyring_file]
[-installFixes <all | recommended | none> ]
```

The **-sharedResourcesDirectory** parameter points to a directory in which Installation Manager will store artifacts from the repository during installation processing. This value is set the first time a product is installed with a particular Installation Manager. You can omit this parameter after the shared resources directory has been set.

If you do not specify the product version to be installed, Installation Manager will install the latest version of the product along with any fixes in the repository locations. You can prevent the installation of fixes by specifying **-installFixes none** or install only recommended fixes by specifying **-installFixes recommended**.

If you specify the product version to be installed, any fixes in the repository locations will only be installed if you specify **-installFixes recommended** or **-installFixes all**.

7. Product installation is complete when the Installation Manager completes without error messages. Logs for the installation can be found in the logs subdirectory of the Installation Manager runtime data location.
8. When product installation is complete, unmount the product file system and remount it read-only for use by Liberty servers.

## Installing IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty

### 8.5.5.5

You can install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty by using IBM Installation Manager Version 1.6.2 or later.

## Before you begin

1. Create an Installation Manager on your z/OS system.  
You need to know the location of the binaries directory for the Installation Manager and have access to a user ID that can invoke the Installation Manager.
2. Install a copy of WebSphere Application Server Liberty for z/OS Version 8.5.5.
3. Obtain the product repository for IBM WebSphere SDK Java Technology Edition Version 8.0. The repository can be mounted read-only.  
You can download the repository for IBM WebSphere SDK Java Technology Edition Version 8.0 from IBM Fix Central.  
For more information about obtaining product repositories, see “Obtaining repositories for installing Liberty on z/OS” on page 1348.

## Procedure

1. Choose the installed copy of WebSphere Application Server Liberty for z/OS Version 8.5.5 onto which you install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty.
2. Mount the product file system for this copy of WebSphere Application Server Liberty for z/OS Version 8.5.5 at the same location at which it was originally installed with IBM Installation Manager.  
The file system requires a minimum of 8,500 tracks (3390) or 400 megabytes of available disk space to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty.  
You can use the `zMountFileSystem.sh` script in the `eclipse/tools` subdirectory of the Installation Manager binaries location to mount this file system. For example:

```
cd /InstallationManager/bin/eclipse/tools
```

```
zMountFileSystem.sh -name WAS.V85.SBBOHFS -type ZFS  
-mountpoint /usr/lpp/zWebSphere/V8R5
```

You can add the **-owner**, **-group**, and **-perm** options to this command to set the ownership and permissions for all files in the file system.

3. Log in to the Unix System Services shell under the Installation Manager user ID, and change the directory to the `eclipse/tools` subdirectory of the Installation Manager binaries location.

For example:

```
cd /InstallationManager/bin/eclipse/tools
```

4. Use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential storage file.

For more information on using the **-secureStorageFile** and **-masterPasswordFile** options, see Installation Manager Version 1.6 documentation.

IBM WebSphere SDK Java Technology Edition Version 8.0:

```
installation_manager_binaries_directory/eclipse/tools/imutilsc saveCredential  
-url http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.IBMJAVA.v80/repository.xml  
-userName user_ID -userPassword user_password  
-secureStorageFile storage_file -masterPasswordFile master_password_file
```

5. Verify that the product repository is available.

You do this verify by issuing the following Installation Manager command-line command.

```
imcl listAvailablePackages -repositories list_of_repository_locations
```

You should see one or more levels of the IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty offering:

- `com.ibm.websphere.liberty.IBMJAVA.v80`

The `list_of_repository_locations` should include the path to the initial product repository and the paths to any additional service repositories. Separate URLs in the `list_of_repository_locations` with commas.

To use the web-based service repository, add the **-useServiceRepository** parameter. For example:

```
imcl listAvailablePackages  
-repositories /usr/lpp/InstallationManagerRepository/HBB0850  
-useServiceRepository  
-secureStorageFile storage_file -masterPasswordFile master_password_file
```

6. Run the Installation Manager command-line tool to install IBM WebSphere SDK Java Technology Edition Version 8.0 for Liberty.

IBM WebSphere SDK Java Technology Edition Version 8.0:

```
imcl install com.ibm.websphere.liberty.IBMJAVA.v80
-installationDirectory installation_location
-repositories list_of_repository_locations
-sharedResourcesDirectory shared_data_location
-acceptLicense
[-useServiceRepository -secureStorageFile storage_file -masterPasswordFile master_password_file]
[-installFixes <all | recommended | none> ]
```

The **-sharedResourcesDirectory** parameter points to a directory in which Installation Manager stores artifacts from the repository during installation processing. This value is set the first time a product is installed with a particular Installation Manager. You can omit this parameter after the shared resources directory has been set.

If you do not specify the product version to be installed, Installation Manager installs the latest version of the product along with any fixes in the repository locations. You can prevent the installation of fixes by specifying **-installFixes none** or install only recommended fixes by specifying **-installFixes recommended**.

If you specify the product version to be installed, any fixes in the repository locations are installed only if you specify **-installFixes recommended** or **-installFixes all**.

7. Product installation is complete when the Installation Manager completes without error messages. Logs for the installation can be found in the logs subdirectory of the Installation Manager runtime data location.
8. When product installation is complete, unmount the product file system and remount it read-only for use by Liberty servers.

## Updating Liberty from Version 8.5.0 to Version 8.5.5

Distributed operating systems

IBM i

8.5.5.0

If you are updating an existing WebSphere Application Server for z/OS Version 8.5.0.x Liberty feature, you must install WebSphere Application Server Liberty for z/OS Version 8.5.5.0 or later. You cannot make an in-place update of the Version 8.5.0.x Liberty feature. Afterwards, you can copy your data and server configurations to the new installation or, if your user data are kept in another location, follow typical procedures for managing your data and server configurations.

### About this task

In WebSphere Application Server Version 8.5.5.0, Liberty was promoted from a feature to an independently installable offering. You cannot make an in-place update of the Version 8.5.0.x Liberty feature. The `wlp` folder includes the Liberty runtime and any user data or server configurations that you have saved in the `wlp/usr` folder. If you have a combined full-profile and Liberty-profile Version 8.5.0.x installation, the update program will back up the `wlp` folder for the existing Version 8.5.0.x Liberty feature into the `wlp.bak_<timestamp>` folder and uninstall the feature during an update to Version 8.5.5.0 or higher. You can continue using Liberty from the backed-up location or copy it elsewhere. To update Liberty to Version 8.5.5.0 or higher, you then must install WebSphere Application Server Liberty for z/OS (with the `com.ibm.websphere.liberty.zOS.v85` offering ID). After installing WebSphere Application Server Liberty for z/OS, you can move any user data and server configurations from the `wlp.bak_<timestamp>` folder to the new Liberty installation.

**Note:** These instructions describe updating from a combined full-profile and Liberty-profile Version 8.5.0.x installation. If you have only the Version 8.5.0.x Liberty feature installed, you should install WebSphere Application Server Liberty for z/OS Version 8.5.5.0 or higher in a different location. Then, you can copy the contents of the `wlp/usr` directory from the old installation to the `usr` directory of the new installation. If you are using `WLP_USER_DIR` and `WLP_OUTPUT_DIR` environment variables, make sure that they are pointing to the desired locations.

## Procedure

1. Update your existing combined full-profile and Liberty-profile installation to Version 8.5.5 or later following the normal update procedure.

After updating your WebSphere Application Server for z/OS installation from Version 8.5.0.x to Version 8.5.5, you can find your Liberty installation in the `<was_home>/wlp.bak_<timestamp>` folder. This backup folder contains the Liberty runtime at the level that it was before you started the update.

2. Use the backed-up Liberty runtime.

A copy of the Installation Manager installation and history information for this snapshot is also stored in the root of the backup in the `installed.xml` and `history.xml` files.

To determine what fixes have been installed in this snapshot, you can use the **bin/productInfo** command in the backed-up Liberty folder. See “Liberty:productInfo command” on page 1415 for more information.

You can continue using the Liberty runtime folder from its backed-up location, or you can copy or move it to a new location. If you have set the `WLP_USER_DIR` or `WLP_OUTPUT_DIR` environment variables, make sure that they point to the location of your user data and the location of output resources generated by your server respectively.

**Note:** Do not move the backed-up `wlp.bak_<timestamp>` folder back to `wlp` in case you decide to roll back to Version 8.5.0.x later.

If `WLP_USER_DIR` has not been set, the server configuration and shared resources are stored in the `usr` directory at the root of the server's runtime environment (`wlp_bak_<timestamp>/usr` for example). In this case, no action is required to use the backed-up runtime because the user data can still be found under the `usr` directory of the new location.

If the `WLP_OUTPUT_DIR` value is not set, the default location is in the server root directory (`wlp_bak_<timestamp>/usr/servers/<server_name>` for example). If this environment variable is not set, no action is required to use the backed up runtime because logs continue to appear under the `usr/servers/<server_name>/logs` directory of the new location.

For more information on these environment variables, see this “Customizing the Liberty environment” on page 1565.

**Note:** If the `server.xml` file or any included XML configuration file references another resource outside the server configuration directory, ensure that these resources can be found from the new server location.

Start all Liberty servers with the **--clean** parameter as a launch option. For example:

```
server start --clean
```

You need to use the **--clean** option only once. All subsequent server starts will not require it.

If you need to apply fixes to the `wlp-bak` follow the instructions in “Applying a fix pack to a Liberty Java archive installation” on page 1380.

3. Install WebSphere Application Server Liberty for z/OS Version 8.5.5 or later.

See “Installing and uninstalling Liberty using Installation Manager” on page 1164 or “Installing and uninstalling Liberty using downloaded files and archives” on page 1371.

4. Start using the WebSphere Application Server Liberty for z/OS Version 8.5.5 installation.

If the `WLP_USER_DIR` and `WLP_OUTPUT_DIR` environment variables are set, then the new Liberty installation will continue using these locations to for user data, including server configurations, and to place server generated output. In this case, it is recommended that you make a backup of the directories referenced by `WLP_USER_DIR` and `WLP_OUTPUT_DIR` before beginning to use the new installation.

If the `WLP_USER_DIR` and `WLP_OUTPUT_DIR` environment variables are not set, Liberty will use folders relative to the installed runtime by default. In this case, you should copy the contents of the backed-up Liberty runtime user folder (`wlp.bak_<timestamp>/usr`) to the `usr` folder of your new installation.

For more information on these environment variables, see this “Customizing the Liberty environment” on page 1565.

**Note:** If the `server.xml` file or any included XML configuration file references another resource outside the server configuration directory, ensure that these resources can be found from the new server location.

## Installing the Extended Programming Models on z/OS

z/OS

8.5.5.4

Installing and updating Liberty with the Extended Programming Models differs depending on the version of WebSphere Application Server.

### About this task

The Extended Programming Models provide a rich set of programming models such as web services, JMS (including Message-driven beans), and MongoDB 2.0.

How you install the Extended Programming Models depends on your version of WebSphere Application Server:

- Up to Version 8.5.5.3: Extended Programming Models are available as the `extprogmodels` Installation Manager installable feature.
- Version 8.5.5.4 and later: Extended Programming Models are available as the `extendedPackage-1.0` Liberty Repository add-on

**Note:** If you are installing or updating to Version 8.5.5.3 or earlier using a remote repository, such as IBM Passport Advantage or a centrally-hosted HTTP server, internet access is required to update the Extended Programming Models.

After you install Liberty Version 8.5.5.4 or later, you can later install the `extendedPackage-1.0` add-on by using the **featureManager** command. For Version 8.5.5.6 and later, you can also use the **installUtility** command to install the add-on from multiple types of repositories. For more information, see “Installing assets using the featureManager command” on page 1403 and “Installing assets using the installUtility command” on page 1393.

### Procedure

Install or update Liberty with the Extended Programming Models using the command line.

- V8.5.5.3 and previous versions install the `extprogmodels` feature after the product:

```
imcl install com.ibm.websphere.liberty.zOS.v85,extprogmodels
-installationDirectory /usr/lpp/zWebSphere/Liberty/V8553 -acceptLicense
-repositories /usr/lpp/InstallationManagerRepository/HBB0850
-sharedResourcesDirectory /InstallationManager/sharedResources
-showProgress
```
- V8.5.5.4 and later versions install the `extendedPackage-1.0` add-on on the **-properties user.addon** parameter:

```
imcl install com.ibm.websphere.liberty.zOS.v85
-properties user.accept.license=true,user.addon=extendedPackage-1.0
-installationDirectory /usr/lpp/zWebSphere/Liberty/V8554 -acceptLicense
-repositories /usr/lpp/InstallationManagerRepository/HBB0850
-sharedResourcesDirectory /InstallationManager/sharedResources
-showProgress
```

## Updating and uninstalling Liberty on z/OS

8.5.5.0

You can use IBM Installation Manager to update or uninstall the WebSphere Application Server Liberty for z/OS offering.

## Optional features

Certain features can be added or removed from an installed copy of the WebSphere Application Server Liberty for z/OS offering. These are called optional features. Choose the optional features for each copy of the WebSphere Application Server Liberty for z/OS code according to your needs.

See “Adding and removing features from Liberty on z/OS.”

## Maintenance

IBM regularly provides updates to the WebSphere Application Server Liberty for z/OS offering to fix defects and add new function. Fix packs contain bundled service to bring WebSphere Application Server Liberty up to a new level. Interim fixes provide updates to correct individual defects. See “Installing Liberty interim fixes and fix packs on z/OS operating systems” on page 1366.

l **New:** Liberty now follows a continuous delivery process with a new fix pack numbering scheme. Fix  
l pack 16.0.0.2 is the next fix pack after 8.5.5.9. You can continue to use the same Version 8.5 Installation  
l Manager repositories and offering IDs to install or update to 16.0.0.2, or you can use the new versionless  
l repositories and offerings. For more information about fix pack 16.0.0.2, see What is new in Liberty in the  
l new location of the latest Liberty documentation.

## Uninstalling the offering

You can use IBM Installation Manager to uninstall individual copies of WebSphere Application Server Liberty for z/OS offering code.

See “Uninstalling the Liberty offering on z/OS” on page 1371.

## Adding and removing features from Liberty on z/OS: **8.5.5.0**

Use IBM Installation Manager to add and remove features for WebSphere Application Server Liberty for z/OS.

### Before you begin

Obtain the product repository for WebSphere Application Server Liberty for z/OS. The following instructions assume that the repository is mounted at `/usr/lpp/InstallationManagerRepository/HBB0850`. The repository can be mounted read-only.

Decide which features you need. Each installed copy of WebSphere Application Server Liberty for z/OS can have a different set of installed features.

The following optional features are available for WebSphere Application Server Liberty for z/OS. The keyword name for each feature is provided in parentheses.

- Embeddable EJB container and JPA client (`embeddablecontainer`)

This option includes the embeddable EJB container and JPA client.

The embeddable EJB container is a Java Archive (JAR) file that you can use to run enterprise beans in a standalone Java Platform, Standard Edition (SE) environment. You can run enterprise beans using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.

The JPA client can be used with the embeddable EJB container to provide Java Persistence API capability in a Java SE environment.

- Extended Programming Models - `extprogmodels` (Version 8.5.5.3 and previous versions)  
The Extended Programming Models feature provides a rich set of programming models such as Web Services, JMS (including Message-Driven Beans), and Mongo 2.0.

### About this task

**8.5.5.4** To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

### Procedure

1. Mount the product file system for the product to which features are being added or removed.
2. Log in to the Unix System Services shell under the Installation Manager user ID, and change the directory to the `eclipse/tools` subdirectory of the Installation Manager binaries location.

For example:

```
cd /InstallationManager/bin/eclipse/tools
```

3. View a list of the features installed with the product.

You do this by issuing the following Installation Manager command-line command:

```
imcl listInstalledPackages -features -long
```

#### Tip:

- When you install a new copy of the WebSphere Application Server Liberty for z/OS and do not specify the features to be installed, the following features are installed by default:
  - `embeddablecontainer`
  - `extprogmodels` (Version 8.5.5.3 and previous versions)

To install the product with a different assortment of features, add a complete list of features that you want (separated by commas) after the package name in the `imcl` install command. For example, the following command:

```
imcl install com.ibm.websphere.liberty.zOS.v85,embeddablecontainer
-installationDirectory installation_location
-repositories list_of_repository_locations
-sharedResourcesDirectory shared_data_location
-acceptLicense
```

would install the product with the `embeddablecontainer` feature.

-  **8.5.5.4** Beginning with Version 8.5.5.4, the `extprogmodels` feature is no longer available. Instead, install the `extendedPackage-1.0` addon, or install the individual features that you need from the Liberty Repository. See the following topics for more information:
    - Installing Liberty Repository assets
    - Liberty features
4. To add one or more features to an existing product installation, issue the `imcl` command and specify the features to be added.

For example:

```
imcl modify com.ibm.websphere.liberty.zOS.v85
-addFeatures embeddablecontainer
-repositories http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.zOS.v85
-installationDirectory installation_location
```

This will add the `embeddablecontainer` feature if it is not already installed.

5. To remove one or more features from an existing product installation, issue the `imcl` command and specify the features to be removed.

For example:

```
imcl modify com.ibm.websphere.liberty.zOS.v85
-removeFeatures embeddablecontainer
-repositories http://www.ibm.com/software/repositorymanager/com.ibm.websphere.liberty.zOS.v85
-installationDirectory installation_location
```

This will remove the `embeddablecontainer` optional feature.

**Note:** Before removing optional features, make sure that none of your applications depend on the features being present.

6. When the appropriate features are added or removed, unmount the product file system and remount it read-only for use by Liberty servers.

## What to do next

Customize or make use of any new features that you added.

## Installing Liberty interim fixes and fix packs on z/OS operating systems: **8.5.5.0**

Fix packs contain bundled service to bring WebSphere Application Server Liberty for z/OS up to a new level. Interim fixes provide corrective service for specific known problems. You can use IBM Installation Manager to update the offering with the fixes that are available for your service level of WebSphere Application Server Liberty for z/OS.

### Before you begin

Contact the IBM Software Support Center for information about updates for WebSphere Application Server Liberty for z/OS. For more information about upgrades, see the *WebSphere Application Server for z/OS: Program Directory*. The most current information is available from the IBM Software Support Center and Fix Central.

**Tip:** Although almost all of the instructions in this section of the information center will work with earlier versions of IBM Installation Manager, the information here is optimized for users who have installed or upgraded to Installation Manager Version 1.5.2 or later.

### About this task

- | **New:** Fix pack 16.0.0.2 is the next fix pack after 8.5.5.9. You can continue to use the same Version 8.5
- | Installation Manager repositories and offering IDs to install or update to 16.0.0.2, or you can use the new
- | versionless repositories and offerings. For more information about fix pack 16.0.0.2, see What is new in
- | Liberty in the new location of the latest Liberty documentation.

**8.5.5.4** To install Version 8.5.5.4 and later of Liberty, you must have IBM Installation Manager Version 1.6.2 or later.

 **8.5.5.4** When fix packs are installed, any installed Liberty features are updated to the new fix pack level. At fix pack level 8.5.5.4 and later, a set of Liberty features at the appropriate level is included in each fix pack repository that is downloaded from Fix Central or installed with SMP/E. When upgrading a copy of Liberty with Liberty features or add-ons, you must add `-properties user.accept.license=true` to the `imcl install` command.

**8.5.5.5** For Version 8.5.5.5 and later, `user.accept.license=true` is not required.

### Procedure

1. Use Installation Manager to apply the required maintenance to your dataset and file-system structure.
  - a. For a list of fixes that are available for WebSphere Application Server Liberty for z/OS and specific information about each fix, perform the following actions.
    - 1) Go to Fix Central.
    - 2) Select **WebSphere** as the product group.
    - 3) Select **WebSphere Application Server Liberty for z/OS** as the product.

- 4) Select the version of the offering to be updated.
  - 5) Select z/OS as the platform, and click **Continue**.
  - 6) Select **Browse for fixes**, and click **Continue**.
  - 7) Click **More Information** under each fix to view information about the fix.
  - 8) **Recommendation:** Make a list of the names of the fixes that you would like to install.
- b. Update WebSphere Application Server Liberty for z/OS with the fixes using one of the following procedures.

- To update the offering with interim fixes or fix packs, access the live service repository that contains the fixes and use web-based updating.

Use Installation Manager on your local system to update WebSphere Application Server Liberty for z/OS with the interim fixes from the live web-based service repositories.

- For the live service repositories, use the same URLs as those used for the generally available product-offering repositories during installation. These URLs are based on the following pattern:

```
http://www.ibm.com/software/repositorymanager/offering_ID
```

where *offering\_ID* is the offering ID that you can find in WebSphere Application Server product offerings for supported operating systems.

- These locations do not contain web pages that you can access using a web browser. They are remote web-based repository locations that you specify for Installation Manager so that it can maintain the offering.

To install a fix from a service repository, perform the following actions:

- 1) Mount the product file system, read and write, at the path at which it was originally mounted with Installation Manager.
- 2) If you do not already have Installation Manager credential-storage and master-password files containing your IBM software user ID and password, create files that will allow you to access the repository.

**Note:** These are the credentials that you use to access protected IBM software websites.

Create a credential-storage file and master-password file:

```
imutilsc saveCredential
  -secureStorageFile storage_file -masterPasswordFile master_password_file
  -userName IBM_software_ID
  -userPassword IBM_software_password
  -url repository_URL
```

**Tip:** When creating a credential-storage file, append */repository.config* at the end of the repository URL location if the **imutilsc** command is unable to find the URL that is specified.

**Note:** When you use Installation Manager Version 1.6.2 and later, you should use the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file. In versions of Installation Manager earlier than Version 1.6.2, the **-keyring** and **-password** options were used to access credentials in a keyring file. These options were deprecated in Version 1.6.2. There is no migration path from keyring files to storage files because of the differences in the file structures. For more information on using the **-secureStorageFile** and **-masterPasswordFile** options to store credentials in a credential-storage file, see the Installation Manager Version 1.6 documentation. For more information on using the **-keyring** and **-password** options to store credentials in a keyring file, see the Installation Manager Version 1.5 documentation.

- 3) From the Installation Manager user ID, perform the following actions:
  - a) Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager.

b) Install the fix.

**To install an interim fix, use this command:**

```
imcl install fix_name
  -installationDirectory offering_installation_location
  -repositories repository_URL
  -secureStorageFile storage_file -masterPasswordFile master_password_file
```

**To install a fix pack, use this command:**

```
imcl install offering_ID_offering_version
  -installationDirectory offering_installation_location
  -repositories repository_URL
  -secureStorageFile storage_file -masterPasswordFile master_password_file
  -acceptLicense
```

**Tips:**

- The *offering\_ID* is the offering ID that is listed in WebSphere Application Server product offerings for supported operating systems.
- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.5.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the `-installFixes` option defaults to all.
  - If the offering version is specified, the `-installFixes` option defaults to none.



**8.5.5.2**

**To install Liberty Repository assets with a fix pack, use this command:**

```
imcl install offering_ID_and_version
  -properties user.feature=feature_shortOrSymbolicName
  -installationDirectory offering_installation_location
  -repositories repository_URL
  -secureStorageFile storage_file -masterPasswordFile master_password_file
  -acceptLicense
```

**Tips:**

- To install assets from the IBM WebSphere Liberty Repository, you must have access to the internet, and you must have IBM Installation Manager Version 1.6.2 or later. For a list of Liberty Repository assets, see the downloads page on WASdev.net.
- If you want to install Liberty Repository features, specify the short names or symbolic names on the **user.feature** option of the **-properties** parameter. Multiple feature names are separated with double commas.
- **8.5.5.4** When upgrading to fix pack 8.5.5.4 or later, the `extprogmodels` install feature is converted to a Liberty addon, `extendedPackage-1.0`. The Liberty Repository must be available to make this upgrade. Also, because this addon has its own license, you must add `-properties user.accept.license=true` to the `imcl install` command. Alternately, you can remove the `extprogmodels` feature before upgrading to fix pack 8.5.5.4; see "Adding and removing features from Liberty on z/OS" on page 1364.

After the upgrade to Version 8.5.5.4, add the extendedPackage-1.0 addon or the specific Liberty features you need; see “Liberty features” on page 826.

- **8.5.5.6** You can also install assets from instances of the Liberty Asset Repository Service or local directory-based repositories. For more information about these asset repositories, see “Installing assets using Installation Manager” on page 1411. Add the repository on the **-repositories** parameter. The repositories are accessed in the order that they are specified. By default, the Liberty Repository is the last of the repositories that are accessed during installation. To disable access to the Liberty Repository, on the **-properties** parameter, set the **user.useLibertyRepository** option to false.

c) **Optional:** List all installed packages to verify the installation:

```
imcl listInstalledPackages -long
```

- To update the offering with interim fixes or fix packs, download the files that contain the fixes from Fix Central and use local updating.

You can download compressed files that contain the fixes from Fix Central. Each compressed fix file contains an Installation Manager repository for the fix and usually has a .zip extension. After downloading the fix files, you can use Installation Manager to update WebSphere Application Server Liberty for z/OS with the fixes.

1) To download the fixes, perform the following actions:

- a) Go to Fix Central.
- b) Select **WebSphere** as the product group.
- c) Select **WebSphere Application Server Liberty for z/OS** as the product.
- d) Select the version of the offering to be updated.
- e) Select z/OS as the platform, and click **Continue**.
- f) Select **Browse for fixes**, and click **Continue**.
- g) Select the fixes that you want to download, and click **Continue**.
- h) Select your download options, and click **Continue**.
- i) Click **I agree** to agree to the terms and conditions.
- j) Click **Download now** to download the fixes.
- k) Transfer the compressed fix files in binary format to the z/OS system on which they will be installed.
- l) If you are installing a fix pack, extract the compressed repository files to a directory on your system.

2) To install a fix from a downloaded file, perform the following actions:

- a) Mount the product file system, read and write, at the path at which it was originally mounted with Installation Manager.
- b) From the Installation Manager user ID, perform the following actions:
  - i. Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager.
  - ii. Install the fix.

**To install an interim fix, use this command:**

```
imcl install fix_name  
-installationDirectory offering_installation_location  
-repositories compressed_file
```

**To install a fix pack, use this command:**

```
imcl install offering_ID_offering_version  
-installationDirectory offering_installation_location  
-repositories location_of_expanded_files  
-acceptLicense
```

**Tips:**

- The *offering\_ID* is the offering ID that is listed in WebSphere Application Server product offerings for supported operating systems.
- The *offering\_version*, which optionally can be attached to the offering ID with an underscore, is a specific version of the offering to install (8.5.5.20110503\_0200 for example).
  - If *offering\_version* is **not** specified, the latest version of the offering and **all** interim fixes for that version are installed.
  - If *offering\_version* is specified, the specified version of the offering and **no** interim fixes for that version are installed.

The offering version can be found attached to the end of the offering ID with an underscore when you run the following command against the repository:

```
imcl listAvailablePackages -repositories source_repository
```

- You can also specify none, recommended or all with the `-installFixes` argument to indicate which interim fixes you want installed with the offering.
  - If the offering version is **not** specified, the `-installFixes` option defaults to all.
  - If the offering version is specified, the `-installFixes` option defaults to none.

iii. **Optional:** List all installed packages to verify the installation:

```
imcl listInstalledPackages -long
```

- To update the offering with fix packs, apply fix-pack PTFs to the SMP/E-managed repository and use local updating.

You can add a new fix-pack level of the offering to the SMP/E-managed repository that contains the base offering by applying PTFs for the fix pack to the repository. See the WebSphere Application Server Liberty for z/OS service page for a listing of available fix packs and PTFs. After installing the PTFs, you can use Installation Manager to update WebSphere Application Server Liberty for z/OS with the new fix pack.

- 1) Apply the PTFs for the fix pack to the WebSphere Application Server Liberty for z/OS repository (FMID HBB0850).
- 2) Perform the following actions:
  - a) Mount the product file system, read and write, at the path at which it was originally mounted with Installation Manager.
  - b) From the Installation Manager user ID, perform the following actions:
    - i. Change to the *Installation\_Manager\_binaries/eclipse/tools* directory, where *Installation\_Manager\_binaries* is the installation root directory for the Installation Manager.
    - ii. Use the **imcl install** command to install the new fix-pack level. For example:

```
imcl install com.ibm.websphere.liberty.z0S.v85_offering_version
-installationDirectory offering_installation_location
-repositories /usr/lpp/InstallationManagerRepository/HBB0850
-acceptLicense
```

**Tips:**

- *offering\_version* can be found attached to the end of the offering ID with an underscore when you run the following command against the repository. For example:

```
imcl listAvailablePackages
-repositories /usr/lpp/InstallationManagerRepository/HBB0850
```

- When the offering is installed for use with WebSphere Application Server Liberty for z/OS, it is installed into the WebSphere Application Server Liberty for z/OS product file system.

iii. **Optional:** List all installed packages to verify the installation:

```
imcl listInstalledPackages -long
```

For more information on updating WebSphere Application Server Liberty for z/OS, see “Updating and uninstalling Liberty on z/OS” on page 1363.

2. Remount the product file system at its production location.

The file system should normally be mounted read-only.

3. Perform any other migration actions as instructed in fix or APAR cover letters.

4. Start your server(s) to complete any necessary post-installation tasks.

At server startup, the post-installer will run automatically against each node in order to update the configuration file system to the new service level.

**Note:** In Network Deployment cells, the deployment manager node must be at the same or a later service level than the cell's application server nodes. You must ensure that the deployment manager node is upgraded to the new service level.

## Uninstalling the Liberty offering on z/OS: **8.5.5.0**

Use IBM Installation Manager to uninstall copies of the product code for WebSphere Application Server Liberty for z/OS, Web Server Plug-ins for IBM WebSphere Application Server for z/OS, or IBM HTTP Server for z/OS.

### Before you begin

Make sure that you no longer need this particular copy of the product code.

### Procedure

1. Mount the file system containing the product code to be uninstalled at the installation location that Installation Manager used to install it.
2. Log in to the Unix System Services shell under the Installation Manager user ID, and change the directory to the `eclipse/tools` subdirectory of the Installation Manager binaries location.

For example:

```
cd /InstallationManager/bin/eclipse/tools
```

3. Invoke the Installation Manager `uninstall` command to perform the product uninstallation.

```
imcl uninstall package_ID  
-installationDirectory installation_location
```

For example:

```
imcl uninstall com.ibm.websphere.liberty.zOS.v85  
-installationDirectory /usr/lpp/zWebSphere/V8R5
```

Product uninstallation is complete when the Installation Manager completes without error messages. Logs for the uninstallation can be found in the `logs` subdirectory of the Installation Manager runtime data location.

4. When product uninstallation is complete, delete any remaining files from the product location.

---

## Installing and uninstalling Liberty using downloaded files and archives

**Distributed operating systems** You can install Liberty by using the WebSphere Application Server Developer Tools for Eclipse, or by extracting an archive file. **z/OS** On the z/OS platform installing Liberty by extracting an archive file is not supported.

**Distributed operating systems** **IBM i**

## About this task

To try out Liberty and use Liberty to develop applications that run on WebSphere Application Server traditional or Liberty, you can download a no-charge, unsupported edition from the WASdev download page.

To use Liberty in a production environment with guaranteed service levels and IBM support, you must purchase WebSphere Application Server (base), WebSphere Application Server Network Deployment, WebSphere Application Server Express, or WebSphere Application Server Liberty Core. Liberty is included with these editions and can also be downloaded separately, as an edition-specific Java archive (JAR) file, from Passport Advantage Online. The associated service is available from Fix Central. If you download and install Liberty from an unsupported JAR or ZIP file, you can later purchase a supported edition and upgrade the license for your existing installation.

The following table lists where you can download each type of installation archive file.

Table 96. Installation archive file locations

File	Content	Passport Advantage Online	IBM Fix Central	WASdev website
JAR files for installing a supported edition-specific V8.5.5.8 or later Liberty runtime environment  Example: wlp-nd-all-8.5.5.x.jar	<b>Runtime</b> Edition-specific, V8.5.5.8 or later  <b>Features</b> All features that apply to that edition		⬆	
ZIP files for installing an unsupported V8.5.5.6 or later Liberty runtime environment with a limited production license  Can be upgraded to a supported edition by using the license upgrade JAR file  Example: wlp-webProfile7-8.5.5.x.zip	<b>Runtime</b> V8.5.5.6 or later  <b>Features</b> Optional Java EE 7 feature sets  <b>SDK</b> Optional IBM Java 8 SDK		⬆	⬆
JAR files for installing an edition-specific V8.5.5.0 Liberty runtime environment  Example: wlp-nd-runtime-8.5.5.0.jar	<b>Runtime</b> Edition-specific, V8.5.5.0  <b>Features</b> V8.5.5.0 features	⬆		

Table 96. Installation archive file locations (continued)

File	Content	Passport Advantage Online	IBM Fix Central	WASdev website
<p>JAR files for installing an edition-specific V8.5.5.1 or later Liberty runtime environment</p> <p>The unsupported JAR file can be upgraded to a supported edition by using the license upgrade JAR file</p> <p>Example: wlp-nd-runtime-8.5.5.6.jar</p>	<p><b>Runtime</b> Edition-specific, V8.5.5.1 or later</p> <p><b>Features</b> Up to the latest levels of the V8.5.5.2 feature set</p>		Fully supported JAR files	Unsupported JAR file only
<p>JAR files for license upgrades:</p> <ul style="list-style-type: none"> <li>• Upgrade trial or unsupported editions to supported editions</li> <li>• Upgrade supported editions to other supported editions with more functionality</li> </ul> <p>Example: wlp-nd-license-8.5.5.jar</p>	No runtime environment or features	△	△	

**Distributed operating systems** For Windows, Linux, and Mac OS, you can also install the WebSphere Application Server Developer Tools for Eclipse, then use the tools to install the profile. For more information, see “Installing Liberty developer tools and (optionally) Liberty” on page 1374.

**Distributed operating systems** IBM i

## Procedure

- **8.5.5.8** You can install Liberty and all features that apply to the edition from a self-extracting JAR file.
  1. Install Liberty from the JAR file.
  2. Optional: Upgrade your product edition or license. For example, you can upgrade from WebSphere Application Server Liberty - Express to WebSphere Application Server Liberty Network Deployment for access to advanced functions.
  3. Update your Liberty installation as needed.
- **8.5.5.6** You can install Liberty and optional features in a single step by extracting an installation ZIP file. Installing Liberty from the ZIP files enables no-charge, unsupported, unlimited use of Liberty in development environments and unsupported limited use in small-scale test and production environments.
  1. Review the available installation ZIP files. You can install only the Liberty kernel with no additional features, or you can install Liberty and a set of features that support application development in certain contexts, such as Java Platform, Enterprise Edition 7.  
If you want to install Liberty and IBM SDK Java Technology Edition Version 8, choose the `wlp-webProfile7-java8-<platform>-<architecture>-<version>.zip` that fits your system.
  2. Install Liberty from the ZIP file. After you install Liberty, you have everything that you need to get started with your chosen set of features.

3. Optional: Install additional Liberty Repository assets by using the **installUtility** command. You can also uninstall any unwanted features.
  4. Optional: Upgrade your Liberty profile to an unlimited production edition. Upgrading your license gives you full access to IBM support in an unlimited test or production environment.
  5. Update your Liberty installation as needed.
- You can install Liberty from a self-extracting JAR file. The JAR files contain the Version 8.5.5.2 feature set, but you can install additional features after you install Liberty.
    1. Install Liberty from the JAR file.
    2. Install Liberty Repository assets.
    3. Optional: Upgrade your product edition or license. For example, you can upgrade from WebSphere Application Server Liberty - Express to WebSphere Application Server Liberty Network Deployment for access to advanced functions.
    4. Update your Liberty installation as needed.

## Installing Liberty developer tools and (optionally) Liberty

### Distributed operating systems

The developer tools for Liberty are available as part of the IBM WebSphere Application Server Developer Tools for Eclipse. In addition, WebSphere Application Server Developer Tools for Eclipse is a lightweight set of tools for developing, assembling, and deploying Java EE, OSGi, Web 2.0, and mobile applications to WebSphere Application Server.

### About this task

To install WebSphere Application Server Developer Tools for Eclipse, see [Installing WebSphere Application Server Developer Tools for Eclipse](#).

### What to do next

After you install the developer tools, you can optionally install WebSphere Application Server Liberty. The developer tools can install Liberty for you when you create a server for the first time. For more information about installing Liberty by using the developer tools, see “Creating a Liberty server by using developer tools” on page 1424.

To learn more about Liberty, see [Liberty overview](#).

## Installing Liberty by extracting a Java archive file

### Distributed operating systems

### IBM i

By running a self-extracting Java archive (JAR) file that contains the distribution image, you can install Liberty and you are ready to create a server.

### Before you begin

Your system must meet the operating system and Java requirements for using Liberty. See [System Requirements for WebSphere Application Server V8.5.5](#).

**IBM i** For the IBM i platform, this topic assumes that the minimum supported Java level is installed at one of the following locations:

- /QOpenSys/QIBM/ProdData/JavaVM/jdk626/32bit
- /QOpenSys/QIBM/ProdData/JavaVM/jdk626/64bit

## Procedure

1. Get a copy of the distribution image JAR file.

- **8.5.5.8** You can download a single, edition-specific archive file that contains the Liberty runtime environment with all applicable features from IBM Fix Central.

These JAR files are called `wlp-edition-all-version.jar`, such as `wlp-nd-all-8.5.5.8.jar`.

- You can download separately packaged archive files that contain the Liberty runtime with the Version 8.5.5.2 feature set.

The edition-specific runtime JAR files are called `wlp-edition-runtime-version.jar`.

- Download the archive file for the no-charge, unsupported edition from the WASdev download page. If you install from this JAR file, you can upgrade later to a supported edition.
- Download the archive file for the initial release, which includes IBM support, from Passport Advantage online. The associated fix packs are available from Fix Central.

If you install a production-licensed edition of the Liberty runtime, you can download and install an archive that contains the programming model extension features. The programming model extensions are packaged as a JAR file called `wlp-extended-version.jar`.

For a list of all available archives, see “Liberty:List of installation Java archive files” on page 1377.

2. Extract the distribution images to your preferred directory.

To extract the distribution image by using the interactive install wizard, run `java -jar wlp-archive-name.jar`. All application server files are stored in subdirectories of the `wlp` directory.

**Note:** If you are installing the separate runtime-only and programming model extensions JAR files, first extract the runtime JAR file, then extract the programming model extensions JAR file.

For a list of the available extraction options, see “Java archive file extraction options” on page 1376.

3. Optional: Set the `JAVA_HOME` property for your environment.

Liberty runs in a Java Runtime Environment (JRE). You can specify the JDK or JRE location using the `JAVA_HOME` property in the `server.env` file, as described in “Customizing the Liberty environment” on page 1565. When you set the `JAVA_HOME` property in the `server.env` file, Liberty uses the same Java runtime location regardless of the user profile that Liberty server runs under.

**IBM i** On the IBM i platform, setting the `JAVA_HOME` property as a system-level environment variable is not recommended. The IBM i platform is a shared environment, and changing system-level environment variables might affect other applications.

**Distributed operating systems** On Linux or UNIX systems, you can instead set `JAVA_HOME` in the user `.bashrc` file, or append the JDK or JRE path to the `PATH` environment variable. On Windows systems, you can instead set `JAVA_HOME` as a system environment variable, or append the JDK or JRE path to the `PATH` system variable. For example, on Windows systems you can use the following commands to set the `JAVA_HOME` property, and to add the Java `/bin` directory to the path:

```
set JAVA_HOME=C:\Progra~1\Java\JDK16
set PATH=%JAVA_HOME%\bin;%PATH%
```

**Note:** **8.5.5.11** Support for using Java SE 6 with WebSphere Liberty ends in September 2017. After the end of support, the Liberty kernel will be recompiled and can no longer run with Java SE 6. If you continue to use Java SE 6 on earlier fix packs after the end of support date, you could expose your environment to security risks.

Java SE 8 is the recommended Java SDK because it provides the latest features and security updates. You can install it by installing the IBM SDK, Java Technology Edition, Version 8 package to the package group that contains WebSphere Liberty.

**Note:** The Liberty runtime environment searches for the `java` command in this order: `JAVA_HOME` property, `JRE_HOME` property, and system `PATH` property.

For more information about supported Java environments, and where to get them, see “Minimum supported Java levels” on page 2333.

4. Optional: Upgrade your Liberty installation to a more advanced supported edition. For example, you can upgrade from WebSphere Application Server Liberty Core to WebSphere Application Server Network Deployment. For more information, see “Upgrading Liberty installations” on page 1386.

## What to do next

After you install Liberty, you can further customize your environment by installing additional assets; see “Installing Liberty Repository assets” on page 1391.

**IBM i** On the IBM i platform, after you extract the distribution image, you can configure all servers to run as jobs in the batch subsystem under the QEJBSVR user profile that is provided with the product. For more information, see “Configuring the Liberty server to start as a job in the QWAS85 subsystem on IBM i” on page 1390.

## Java archive file extraction options

You can install Liberty by extracting a Java archive (JAR) file. By running a self-extracting JAR file that contains the distribution image, you can install Liberty and you are ready to create a server.

**8.5.5.0** You can also install programming model extensions by extracting a JAR file.

### Syntax

The command syntax is as follows:

```
java -jar archive-file-name.jar [Options] [install location]
```

where *archive-file-name.jar* is the name of the archive file you are extracting.

### Note:

- If you do not specify any options, the distribution image is extracted by using the interactive installer.
- If you do not specify an installation location, the default target directory is the location of the archive file.

## Options

The following options are available for the extraction command:

**--help** Display a short explanation about how to use the command and a list of available options

**--acceptLicense**  
Automatically indicate acceptance of license terms and conditions

**--verbose**  
Display detailed information during archive extraction

**--viewLicenseAgreement**  
View license agreement

**--viewLicenseInfo**  
View license information

## Usage

The following examples demonstrate the correct syntax:

```
java -jar myarchivefile.jar
java -jar myarchivefile.jar --help
java -jar myarchivefile.jar --acceptLicense C:\Liberty-install
java -jar myarchivefile.jar --verbose
java -jar myarchivefile.jar --viewLicenseAgreement
java -jar myarchivefile.jar --viewLicenseInfo
```

## Liberty:List of installation Java archive files

**8.5.5.0**

You can install Liberty by extracting a Java archive (JAR) file.

**Note:** **8.5.5.6** You can alternatively install Liberty and optional features from the installation ZIP files. For more information, see “Installing Liberty by extracting a ZIP archive file” on page 1381.

**8.5.5.8** Java archive files that contain all applicable features

The following JAR files contain the Liberty runtime and all features that apply to the specific edition.

### WebSphere Application Server Network Deployment

wlp-nd-all-<version>.jar

The WebSphere Application Server Network Deployment Liberty runtime environment and all Liberty features that apply to the edition.

### WebSphere Application Server (base)

wlp-base-all-<version>.jar

The single-server WebSphere Application Server Liberty runtime environment and all Liberty features that apply to the edition.

### WebSphere Application Server Liberty Core

wlp-core-all-<version>.jar

The WebSphere Application Server Liberty Core runtime environment and all Liberty features that apply to the edition.

## Java archive files that contain the Version 8.5.5.2 feature set

The following JAR files contain up to the Version 8.5.5.2 feature set at the latest level of code for the fix pack that you install. You can install additional assets from the Liberty Repository. For more information, see “Installing Liberty Repository assets” on page 1391.

### WebSphere Application Server Network Deployment

**wlp-nd-runtime-<version>.jar**

Liberty for the WebSphere Application Server Network Deployment edition.

**wlp-extended-<version>.jar**

Programming model extensions, licensed for use in production on any production licensed edition other than WebSphere Application Server Liberty Core. Before you can install wlp-extended-<version>.jar, you must install a production licensed edition of Liberty, other than WebSphere Application Server Liberty Core. For a list of the features provided by the programming model extensions archive, see Extended Programming Models.

**wlp-extras-<version>.jar**

The embeddable EJB Container, and JPA client, to help with developing and testing EJB Lite and JPA applications. You must install this JAR file in an empty directory.

## WebSphere Application Server for Developers (IPLA)

### wlp-developers-runtime-ipla-*<version>*.jar

The production (IPLA) licensed Liberty for the WebSphere Application Server for Developers edition.

### wlp-extended-*<version>*.jar

Programming model extensions, licensed for use in production on any production licensed edition other than WebSphere Application Server Liberty Core. Before you can install wlp-extended-*<version>*.jar, you must install a production licensed edition of Liberty, other than WebSphere Application Server Liberty Core. For a list of the features provided by the programming model extensions archive, see Extended Programming Models.

### wlp-extras-*<version>*.jar

The embeddable EJB Container, and JPA client, to help with developing and testing EJB Lite and JPA applications. You must install this JAR file in an empty directory.

## WebSphere Application Server for Developers (ILAN)

### wlp-developers-runtime-*<version>*.jar

The developer licensed Liberty for the WebSphere Application Server for Developers edition.

### wlp-developers-extended-*<version>*.jar

Programming model extensions, licensed for use in development on the WebSphere Application Server for Developers edition. Before you can install wlp-developers-extended-*<version>*.jar, you must install Liberty for the WebSphere Application Server for Developers edition.

### wlp-developers-extras-*<version>*.jar

The embeddable EJB Container, and JPA client, to help with developing and testing EJB Lite and JPA applications. You must install this JAR file in an empty directory.

## WebSphere Application Server Network Deployment trial

### wlp-nd-runtime-trial-*<version>*.jar

Liberty for the WebSphere Application Server Network Deployment edition, licensed for trial use.

## Features included in the JAR files

The following table compares the features that are included in the JAR files that contain the Version 8.5.5.2 feature set. For more information about these features, see “Liberty features” on page 826.

Table 97. Features included in the JAR files

Feature	WebSphere Application Server Liberty Core	WebSphere Application Server (base)	WebSphere Application Server Express	WebSphere Application Server Network Deployment	WebSphere Application Server for Developers (IPLA and ILAN)
Runtime JAR files	wlp-core-runtime- <i>&lt;version&gt;</i> .jar wlp-core-trial-runtime- <i>&lt;version&gt;</i> .jar	wlp-base-runtime- <i>&lt;version&gt;</i> .jar wlp-base-trial-runtime- <i>&lt;version&gt;</i> .jar wlp-runtime- <i>&lt;version&gt;</i> .jar	wlp-express-runtime- <i>&lt;version&gt;</i> .jar wlp-express-trial-runtime- <i>&lt;version&gt;</i> .jar	wlp-nd-runtime- <i>&lt;version&gt;</i> .jar wlp-nd-trial-runtime- <i>&lt;version&gt;</i> .jar	wlp-developers-runtime-ipla- <i>&lt;version&gt;</i> .jar wlp-developers-runtime-ilan- <i>&lt;version&gt;</i> .jar
Java EE 6 Web Profile					

Table 97. Features included in the JAR files (continued)

Feature	WebSphere Application Server Liberty Core	WebSphere Application Server (base)	WebSphere Application Server Express	WebSphere Application Server Network Deployment	WebSphere Application Server for Developers (IPLA and ILAN)
beanValidation-1.0 cdi-1.0 ejbLite-3.1 jaxrs-1.1 jdbc-4.0 jndi-1.0 jpa-2.0 jsf-2.0 json-1.0 jsp-2.2 managedBeans-1.0 servlet-3.0 webProfile-6.0	△	△	△	△	△
<b>Enterprise OSGi</b>					
blueprint-1.0 osgi.jpa-1.0 wab-1.0	△	△	△	△	△
<b>Operations</b>					
appSecurity-1.0 appSecurity-2.0 distributedMap-1.0 ldapRegistry-3.0 localConnector-1.0 monitor-1.0 oauth-2.0 osgiConsole-1.0 restConnector-1.0 serverStatus-1.0 sessionDatabase-1.0 ssl-1.0 timedOperations-1.0 webCache-1.0	△	△	△	△	△
<b>Systems Management</b>					
clusterMember-1.0 collectiveController-1.0				△	
collectiveMember-1.0 concurrent-1.0	△	△	△	△	△
<b>Extended Programming Model JAR files</b>					
N/A		wlp-extended-<version>.jar	wlp-express-extended-<version>.jar	wlp-network-extended-<version>.jar	wlp-developers-extended-<version>.jar

Table 97. Features included in the JAR files (continued)

Feature	WebSphere Application Server Liberty Core	WebSphere Application Server (base)	WebSphere Application Server Express	WebSphere Application Server Network Deployment	WebSphere Application Server for Developers (IPLA and ILAN)
jaxb-2.2 jaxws-2.2 jmsMdb-3.1 mongodb-2.0 wasJmsClient-1.1 wasJmsSecurity-1.0 wasJmsServer-1.0 wmqJmsClient-1.1 wsSecurity-1.1		△	△	△	△

## Applying a fix pack to a Liberty Java archive installation

Distributed operating systems

IBM i

Liberty offers a self-extracting Java archive-based installation as an alternative to using IBM Installation Manager. If you installed Liberty by using the self-extracting archive, and want to upgrade to the latest fix pack version, you can apply a new fix pack archive to a new location, then move any required user files and server configuration data.

### About this task

If you used IBM Installation Manager to install Liberty, you must use Installation Manager to apply a fix pack.

**Important:** You must apply a new fix pack archive to a new location.

### Procedure

1. Install the new runtime environment.
  - a. Copy or download the new fix pack archive onto the target system.
  - b. Launch the archive by using a Java command. You must use a Java command because the archive is an executable JAR file. Run the following command:
    - `java -jar <downloaded_archive_location>/<downloaded_archive_file_name>`

For more information about using a Java command to launch an archive, see the instructions in “Installing Liberty by extracting a Java archive file” on page 1374.
  - c. Review the license terms, and accept them to continue with the installation.
  - d. Select the installation location. Use a different location to where the previous version is installed.
2. Move any user data and server configurations. Liberty defines two locations for storing user-generated content and server configurations:
  - WLP\_USER\_DIR; The location of server configuration files, including shared resources.
  - WLP\_OUTPUT\_DIR; The location of resources generated by the server. For example, log files and temporary disk storage.

If the WLP\_USER\_DIR environment variable has been set on your system, then the new runtime environment will continue to use the same location. This results in no backup of server configuration data. To ensure that your server configuration is backed up, copy the directory referenced by WLP\_USER\_DIR to a new location on your file system. To protect the original environment, change the value of WLP\_USER\_DIR to point to the new location. During uninstallation, reset the value of WLP\_USER\_DIR to the location of the original server configuration.

If WLP\_USER\_DIR has not been set, the server configuration and shared resources are stored in the usr directory at the root of the server's runtime environment (for example, `<liberty_server_runtime_root>/usr`). During uninstallation of the runtime environment, you can reset the WLP\_USER\_DIR environment variable.

If the WLP\_OUTPUT\_DIR environment variable is set on your system, the new server also uses this location. This can result in old log files being overwritten. To ensure that old log files are protected, either update or unset the WLP\_OUTPUT\_DIR environment variable. During uninstallation, reset this value to its original value.

If the WLP\_OUTPUT\_DIR value is not set, the default location is in the server root directory (for example `<liberty_server_runtime_root>/usr/servers/<serverName>`). If the new runtime environment is installed to a new location, no updates are required during installation or uninstallation because logs continue to appear under the `usr/servers/<serverName>/logs` directory of each respective installation.

**Note:** If the `server.xml` file, or any included XML configuration file, references another resource outside the server configuration directory, these resources must also be copied across, or the references will need to be updated. This also applies to any resources that the application references directly, such as references to hardcoded paths on file systems. During uninstallation of the fix pack, these values can be manually reset to their original values.

3. Start the new server. Run `<liberty_VX+>/bin/server start <server_name>`.

### Removing a fix pack from a Liberty Java archive installation:

Distributed operating systems

IBM i

If you installed Liberty by using the self-extracting Java archive, you can uninstall a fix pack from the Liberty runtime environment in a given location by migrating any user data and server configurations to the previous Liberty profile runtime environment in a different location, and deleting the fix pack runtime environment.

#### Procedure

1. Stop all servers running on the system.
  - `<liberty_VX>/bin/server stop <server_name>`
2. Move any user data and server configurations. For more information see the Move any user data and server configurations step in the installation task.
3. Delete the fix pack runtime environment.
4. Start the servers.
  - `<liberty_VX->/bin/server start <server_name>`

## Installing Liberty by extracting a ZIP archive file

Distributed operating systems

IBM i

8.5.5.6

You can install Liberty and optional features by extracting a ZIP archive file. These ZIP files are designed to help you quickly get started with Liberty.

### Before you begin

Your system must meet the operating system and Java requirements for using Liberty. See System Requirements for WebSphere Application Server V8.5.5.

**IBM i** For the IBM i platform, this topic assumes that the minimum supported Java level is installed at one of the following locations:

- `/QOpenSys/QIBM/ProdData/JavaVM/jdk626/32bit`
- `/QOpenSys/QIBM/ProdData/JavaVM/jdk626/64bit`

## About this task

Installing Liberty from the ZIP files enables no-charge, unsupported, unlimited use of Liberty in development environments and limited use in small-scale test and production environments. For more information, see the license information and license agreement files in the `wlp\laf\files` directory or WASdev.net. For access to IBM support and unlimited test and production use, you can later purchase and upgrade to a supported edition from your existing installation.

You can choose from several ZIP files to fit your needs:

- Java Platform, Enterprise Edition (Java EE) 7 technologies: Install the Liberty runtime environment plus features that support the Java EE 7 full platform, Web Profile, or application client
- IBM Java 8: Install the Liberty runtime environment, features that support the Java EE 7 Web Profile, and IBM SDK Java Technology Edition Version 8
- **8.5.5.9** OSGi technologies: Install the Liberty runtime environment and features that support the Java EE 7 Web Profile and OSGi
- Liberty kernel only: Install only the Liberty runtime environment

For a list of the available ZIP archive files, see “Liberty: List of installation ZIP archive files” on page 1383.

 **Watch:** Video: Installing Liberty from a ZIP file shows how you can quickly install Liberty from a ZIP archive file, start the server and add applications, and upgrade to a supported installation [Transcript]

## Procedure

1. Download the ZIP file of the distribution image from Fix Central or the product asset page on WASdev.net. The `wlp-<name>-<version>.zip` files contain logical groupings of features.
2. Extract the distribution image to your preferred directory. All of the application server files are stored in subdirectories of the `wlp` directory.
3. Optional: Set the **JAVA\_HOME** property for your environment.

Liberty runs in a Java Runtime Environment (JRE). You can specify the JDK or JRE location using the **JAVA\_HOME** property in the `server.env` file, as described in “Customizing the Liberty environment” on page 1565. When you set the **JAVA\_HOME** property in the `server.env` file, Liberty uses the same Java runtime location regardless of the user profile that Liberty server runs under.

**IBM i** On the IBM i platform, setting the **JAVA\_HOME** property as a system-level environment variable is not recommended. The IBM i platform is a shared environment, and changing system-level environment variables might affect other applications.

**Distributed operating systems** On Linux or UNIX systems, you can instead set **JAVA\_HOME** in the user `.bashrc` file, or append the JDK or JRE path to the **PATH** environment variable. On Windows systems, you can instead set **JAVA\_HOME** as a system environment variable, or append the JDK or JRE path to the **PATH** system variable. For example, on Windows systems you can use the following commands to set the **JAVA\_HOME** property, and to add the Java `/bin` directory to the path:

```
set JAVA_HOME=C:\Progra~1\Java\JDK16
set PATH=%JAVA_HOME%\bin;%PATH%
```

**Note:** **8.5.5.11** Support for using Java SE 6 with WebSphere Liberty ends in September 2017. After the end of support, the Liberty kernel will be recompiled and can no longer run with Java SE 6. If you continue to use Java SE 6 on earlier fix packs after the end of support date, you could expose your environment to security risks.

Java SE 8 is the recommended Java SDK because it provides the latest features and security updates. You can install it by installing the IBM SDK, Java Technology Edition, Version 8 package to the package group that contains WebSphere Liberty.

**Note:** The Liberty runtime environment searches for the **java** command in this order: **JAVA\_HOME** property, **JRE\_HOME** property, and system **PATH** property.

For more information about supported Java environments, and where to get them, see “Minimum supported Java levels” on page 2333.

4. Optional: Upgrade your Liberty installation to an unlimited production edition. Upgrading your license gives you full access to IBM support in an unlimited test or production environment. For more information, see “Upgrading Liberty installations” on page 1386.

## What to do next

After you install Liberty from a ZIP file, you can further customize your environment by installing additional assets; see “Installing Liberty Repository assets” on page 1391.

**IBM i** On the IBM i platform, after you extract the distribution image, you can configure all servers to run as jobs in the batch subsystem under the QEJBSVR user profile that is provided with the product. For more information, see “Configuring the Liberty server to start as a job in the QWAS85 subsystem on IBM i” on page 1390.

## Liberty: List of installation ZIP archive files

Distributed operating systems

IBM i

8.5.5.6

You can install Liberty by extracting a ZIP archive file. After you install Liberty, you can install additional features by using the **installUtility** command.

The following sections list Liberty ZIP archive files. For more information about each ZIP file, see the related product asset description on the WASdev community download page.

### WAS Liberty V8.5.5.x Kernel

**wlp-kernel-*<version>*.zip**

This basic ZIP file includes only the kernel of the Liberty server and no features.

### WAS Liberty V8.5.5.x with Java EE 7 Web Profile

**wlp-webProfile7-*<version>*.zip**

This ZIP file includes the Liberty server runtime environment and features that support the Java EE 7 Web Profile.

**wlp-webProfile7-java8-*<platform>*-*<architecture>*-*<version>*.zip**

These ZIP files include the Liberty server runtime environment, IBM SDK Java Technology Edition Version 8, and features that support the Java EE 7 Web Profile. There are individual ZIP files for each available platform and architecture. You can later update the IBM Java SDK; for more information, see “Updating the Java software development kit in a Liberty ZIP archive installation” on page 1386.

### WAS Liberty V8.5.5.x with Java EE 7 Full Platform

**wlp-javaee7-*<version>*.zip**

This ZIP file includes the Liberty server runtime environment and features that support Java EE 7.

### WAS Liberty V8.5.5.x with Java EE 7 Application Client

**wlp-javaeeClient7-*<version>*.zip**

This ZIP file includes the Liberty server runtime environment and the Java EE 7 application client.

## WAS Liberty V8.5.5.x with OSGi Applications

### wlp-osgi-<version>.zip

This ZIP file includes the Liberty server runtime environment and features that support OSGi applications.

### Features included in the installation ZIP files

The following table compares the features that are included in each of the available ZIP files. For more information about these features, see “Liberty features” on page 826.

Table 98. Features that are included in the installation ZIP files

Feature	WAS Liberty V8.5.5.x Kernel	WAS Liberty V8.5.5.x with Java EE 7 Web Profile	WAS Liberty V8.5.5.x with Java EE 7 Full Platform	WAS Liberty V8.5.5.x with Java EE 7 Application Client	WAS Liberty with Micro profile	WAS Liberty V8.5.5.x with OSGi Applications
webProfile-7.0		△				
javaee-7.0			△			
appSecurityClient-1.0 javaeeClient-7.0			△	△		
blueprint-1.0 distributedMap-1.0 el-3.0 jaxrs-2.0 jdbc-4.1 jndi-1.0 jpa-2.1 jsf-2.2 jsonp-1.0 jsp-2.3 osgiBundle-1.0 sessionDatabase-1.0 servlet-3.1 websocket-1.1						△
appSecurity-2.0 collectiveMember-1.0 ldapRegistry-3.0 localConnector-1.0 monitor-1.0 requestTiming-1.0 restConnector-1.0 ssl-1.0 webCache-1.0		△	△			△

## Applying a fix pack to a Liberty ZIP archive installation

Distributed operating systems

IBM i

8.5.5.6

Liberty offers a ZIP archive-based installation as an alternative to using IBM Installation Manager. If you installed Liberty from the ZIP archive file and want to upgrade to the latest fix pack version, you can apply a new fix pack archive to a new location, and move any required user files and server configuration data.

## About this task

If you used IBM Installation Manager to install Liberty, you must use Installation Manager to apply a fix pack.

**Important:** You must apply a new fix pack archive to a new location.

## Procedure

1. Install the new runtime environment by downloading the ZIP archive file from WASdev.net and extracting it. For more information, see “Installing Liberty by extracting a ZIP archive file” on page 1381.
2. Optional: Upgrade the new installation to an edition with advanced functionality. If you upgraded your previous installation, upgrade to a product edition with at least the same level of functionality to reduce the chance of any incompatibilities. For example, if you previously upgraded to WebSphere Application Server Liberty (base), upgrade to that same edition or WebSphere Application Server Liberty Network Deployment. For more information, see “Upgrading Liberty installations” on page 1386.
3. Optional: Install Liberty Repository assets to customize the new environment. For more information, see “Installing Liberty Repository assets” on page 1391.
4. Move any user data and server configurations. Liberty defines two locations for storing user-generated content and server configurations:
  - WLP\_USER\_DIR; The location of server configuration files, including shared resources.
  - WLP\_OUTPUT\_DIR; The location of resources generated by the server. For example, log files and temporary disk storage.

If the WLP\_USER\_DIR environment variable has been set on your system, then the new runtime environment will continue to use the same location. This results in no backup of server configuration data. To ensure that your server configuration is backed up, copy the directory referenced by WLP\_USER\_DIR to a new location on your file system. To protect the original environment, change the value of WLP\_USER\_DIR to point to the new location. During uninstallation, reset the value of WLP\_USER\_DIR to the location of the original server configuration.

If WLP\_USER\_DIR has not been set, the server configuration and shared resources are stored in the `usr` directory at the root of the server's runtime environment (for example, `<liberty_server_runtime_root>/usr`). During uninstallation of the runtime environment, you can reset the WLP\_USER\_DIR environment variable.

If the WLP\_OUTPUT\_DIR environment variable is set on your system, the new server also uses this location. This can result in old log files being overwritten. To ensure that old log files are protected, either update or unset the WLP\_OUTPUT\_DIR environment variable. During uninstallation, reset this value to its original value.

If the WLP\_OUTPUT\_DIR value is not set, the default location is in the server root directory (for example `<liberty_server_runtime_root>/usr/servers/<serverName>`). If the new runtime environment is installed to a new location, no updates are required during installation or uninstallation because logs continue to appear under the `usr/servers/<serverName>/logs` directory of each respective installation.

**Note:** If the `server.xml` file, or any included XML configuration file, references another resource outside the server configuration directory, these resources must also be copied across, or the references will need to be updated. This also applies to any resources that the application references directly, such as references to hardcoded paths on file systems. During uninstallation of the fix pack, these values can be manually reset to their original values.

5. Start the new server. Run `<liberty_VX+>/bin/server start <server_name>`.

## What to do next

After you verify that the new installation works correctly, you can remove the old installation. In the previous installation, stop all servers, then delete the wlp directory.

## Updating the Java software development kit in a Liberty ZIP archive installation

Distributed operating systems

IBM i

8.5.5.6

If you installed Liberty with IBM SDK, Java Technology Edition, Version 8 by extracting a ZIP archive file, you can update the Java software development kit (SDK) to incorporate Java service releases and interim fixes.

### About this task

The directories in the following procedures are based on Liberty installations that were installed by extracting a wlp-webProfile7-java8-*<platform>-<architecture>-<version>*.zip file, available from IBM Fix Central or WASdev.net. If you separately installed or moved the IBM Java SDK to a different location, you can update the SDK by replacing the files at their current location.

### Procedure

8.5.5.7 For Version 8.5.5.7 or later:

- Update the Java SDK in a Liberty ZIP archive installation.
  1. Download the IBM SDK, Java Technology Edition, Version 8 ZIP archive file from IBM Fix Central. If you are applying a Java service release or interim fix that is associated with a certain APAR, see the APAR text for download information.
  2. Extract the Java SDK ZIP archive file to a local directory.
  3. Back up the wlp/java/java directory in your Liberty installation by renaming the folder. For example, rename the wlp/java/java directory to wlp/java/java\_backup.
  4. Copy the sdk folder from the directory where you extracted the Java SDK ZIP archive file to the wlp/java directory. Rename the new wlp/java/sdk directory to wlp/java/java.

8.5.5.6 For Version 8.5.5.6 only:

- Update the Java SDK in a Liberty ZIP archive installation.
  1. Download the IBM SDK, Java Technology Edition, Version 8 ZIP archive file from IBM Fix Central. If you are applying a Java service release or interim fix that is associated with a certain APAR, see the APAR text for download information.
  2. Extract the Java SDK ZIP archive file to a local directory.
  3. Back up the wlp/java directory in your Liberty installation by renaming the folder. For example, rename the wlp/java directory to wlp/java\_backup.
  4. Copy the sdk folder from the directory where you extracted the Java SDK ZIP archive file to the wlp directory. Rename the new wlp/sdk directory to wlp/java.
  5. Copy the java.env file from the wlp/java\_backup backup directory to the wlp/java directory.

## What to do next

After you verify that IBM SDK, Java Technology Edition, Version 8 updated successfully, delete the Java backup directory.

## Upgrading Liberty installations

Distributed operating systems

IBM i

8.5.5.5

You can upgrade the edition or license of Liberty by using a self-extracting Java archive (JAR) file.

## Before you begin

To download the upgrade JAR files from IBM Fix Central or Passport Advantage, you must be enrolled as a customer.

Your system must meet the operating system and Java requirements for using Liberty. See System Requirements for WebSphere Application Server V8.5.5.

**IBM i** For the IBM i platform, the minimum supported Java level is installed at one of the following locations:

- /QOpenSys/QIBM/ProdData/JavaVM/jdk626/32bit
- /QOpenSys/QIBM/ProdData/JavaVM/jdk626/64bit

## About this task

Liberty offers installation from a ZIP archive file or a self-extracting Java archive (JAR) file as an alternative to using IBM Installation Manager. If you installed Liberty using one of these archive files, you can upgrade the product license by applying an executable JAR file, available from IBM Fix Central or the Passport Advantage website.

You might upgrade Liberty in the following example scenarios:

- Upgrade a trial edition or other unsupported edition to a supported production edition.
- Upgrade a basic edition to a more advanced edition for access to advanced features.

You can upgrade WebSphere Application Server Liberty offerings in the following paths:

*Table 99. Liberty offering upgrade paths*

License JAR file	Source edition	Target edition
wlp-core-license.jar	Unsupported ZIP or JAR file installations WebSphere Application Server Liberty Core Trial	WebSphere Application Server Liberty Core
wlp-base-license.jar	Unsupported ZIP or JAR file installations WebSphere Application Server Liberty Trial WebSphere Application Server Liberty Core WebSphere Application Server Liberty for Developers WebSphere Application Server Liberty - Express	WebSphere Application Server Liberty

Table 99. Liberty offering upgrade paths (continued)

License JAR file	Source edition	Target edition
wlp-nd-license.jar	Unsupported ZIP or JAR file installations WebSphere Application Server Liberty Network Deployment Trial WebSphere Application Server Liberty Core WebSphere Application Server Liberty for Developers WebSphere Application Server Liberty - Express WebSphere Application Server Liberty	WebSphere Application Server Liberty Network Deployment

For example, an installation of WebSphere Application Server Liberty Core also requires features from WebSphere Application Server Network Deployment. If you have the required entitlement, you can download the `wlp-nd-license.jar` license file and apply it to your Liberty installation, which upgrades the license from WebSphere Application Server Liberty Core to WebSphere Application Server Network Deployment. Upgrading the license does not install any features from WebSphere Application Server Network Deployment, but it enables you to install WebSphere Application Server Network Deployment features to your Liberty installation if needed.

## Procedure

1. Download the license upgrade archive for the edition that you want to upgrade to from IBM Fix Central or the IBM Passport Advantage website. You can apply the license JAR files to all fix packs of Liberty ZIP or JAR file installations.

For a list of the JAR files on IBM Fix Central, see license JAR files on the Fix Central website.

For a list of Passport Advantage part numbers, see How to download WebSphere Application Server Network Deployment V8.5.5 from Passport Advantage Online.

2. Apply the license archive to an existing Liberty installation. For example, to apply the license by using the installation wizard and the `wlp-nd-license.jar` file, run the following command:

```
java -jar wlp-nd-license.jar
```

## Applying an interim fix to a Liberty archive installation

Distributed operating systems

IBM i

Liberty offers a self-extracting archive-based installation as an alternative to using IBM Installation Manager. If you installed Liberty using the self-extracting archive, and want to install an interim fix, you can apply an executable JAR file.

### About this task

If you used IBM Installation Manager to install Liberty, you must use Installation Manager to apply an interim fix.

An archive-based interim fix is named `<Liberty profile level>-WS-WASProd_WLPArchive-<fix type><fix id>.jar`

- `<Liberty profile level>` refers to a 4-digit fix pack level identifier, which indicates the minimum level to which the fix applies. For example, 8.5.5.0.
- `<fix type>` refers to the type of fix. For example, IF is used for an interim fix, and TF for a diagnostic fix

- *<fix id>* refers to the APAR reference number. If a diagnostic fix is provided before an APAR is opened, the *<fix id>* is based on the PMR reference number.

Each interim fix is installed by executing the relevant JAR file, which extracts the content into the Liberty base folder (/wlp).

**Note:** When the interim fix is applied, no backup data is created. If you want to back out an interim fix, you must manually remove or restore files from the /wlp folder.

Each interim fix is provided with a `readme.txt` file, which contains backup and restore instructions specific to the fix content, in a section titled **Directions to apply fix**. If the `readme.txt` file does not specify any requirement to back up files, you can extract the fix and then restart the server at any time with the `--clean` parameter as a launch option.

## Procedure

1. Optional: If the fix contains files that will overwrite existing files, stop all servers that are running on the system.
2. Optional: If the `readme.txt` file indicates that a backup is required, create a backup of the `lib/features/component.mf` files. File locations are relative to your Liberty profile installation root.
3. Open a console and direct it to the location of your interim fix JAR file.
4. To view available options, run `java -jar interim_fix_jar_file -help`, where *interim\_fix\_jar\_file* is the name of the executable JAR file that contains the interim fix. The following launch options are available for the JAR file:

### `--installLocation [LibertyRootDir]`

The absolute or relative location of the Liberty installation directory.

By default the JAR file looks for a `wlp` directory in its current location. If your Liberty profile installation location is not the `wlp` folder, or is not in the same directory as the JAR file, then you can use this option to change where the JAR file will patch. `[LibertyRootDir]` can either be relative to the location of the JAR file, or an absolute file path.

### `--suppressInfo`

The only messages output from the JAR file will be error messages or confirmation that patching is complete.

5. Run the JAR file, using the `--installLocation` option to specify the installation location. For example, `java -jar interim_fix_jar_file --installLocation`. Optionally include `--suppressInfo`.
6. Start all Liberty profile servers with the `--clean` parameter as a launch option. For example, `server start --clean`. You use the `--clean` option only once; all subsequent server starts do not require it.

## Removing an interim fix from a Liberty archive install

Distributed operating systems

IBM i

If you installed Liberty by using the self-extracting archive, then to remove an interim fix you must manually remove files, and restore files, from the /wlp folder.

### About this task

If you used IBM Installation Manager to apply an interim fix, you can use Installation Manager to remove the interim fix.

The current set of fixes installed on a Liberty profile can be found in the `/lib/fixes` directory.

Each interim fix is provided with a `readme.txt` file, which contains backup and restore instructions specific to the fix content, in a section titled **Directions to apply fix**. If the `readme.txt` file does not

include any requirement to back up files, you can extract the fix and then restart the server at any time with the `--clean` parameter as a launch option.

## Procedure

1. Stop all servers running on the system. For more information, see Starting and stopping a server.
2. Delete or replace the files as detailed in the `readme.txt` file. File locations are relative to your Liberty profile install root. For example:
  - `lib/com.ibm.ws.component_1.0.0.20120803-1356.jar`
  - `lib/fixes/8.5.0.0-WASProd_WLPArchive-IFPM11111_8.5.0.20120803-1356.xml`
3. Start all Liberty profile servers with the `--clean` parameter as a launch option. For example, `server start --clean`. You only need to use the `--clean` option once. All subsequent server starts will not require it.

## What to do next

You can reapply the fix by following the instructions in “Applying an interim fix to a Liberty archive installation” on page 1388.

## Configuring the Liberty server to start as a job in the QWAS85 subsystem on IBM i

IBM i

You can optionally use the `iAdmin POSTINSTALL` command to configure the Liberty server to start as a job in the QWAS85 subsystem and to run under the `QEJBSVR` user profile.

### About this task

The `iAdmin POSTINSTALL` command configures the server start command to start servers as jobs in the QWAS85 subsystem. Additionally, the task can be used to:

- Configure Liberty to run servers under the `QEJBSVR` user profile.
- Configure the default JDK location by setting `WLP_DEFAULT_JAVA_HOME` in file `wlp/etc/default.env` to the location of the 32 bit version of the minimum supported Java level.
- Add an entry for the product in the IBM i native product registry.
- Create IBM i native libraries and objects such as the QWAS85 subsystem and the `QEJBSVR` user profile.

Call the `iAdmin POSTINSTALL` command only after Installing Liberty by extracting an archive file.

**Note:** You must have `*ALLOBJ` and `*SECADM` special authority to use the `iAdmin POSTINSTALL` command.

### Procedure

1. On the IBM i command line, run the `STRQSH` command to start the Qshell.
2. In the resulting Qshell session, change the directory to the `wlp` directory.
3. Run the following command.

```
lib/native/os400/bin/iAdmin POSTINSTALL
```

## Uninstalling Liberty application-serving environment from IBM i operating systems

IBM i

By calling the iAdmin PREUNINSTALL command, you can remove any IBM i native objects and libraries created by the iAdmin POSTINSTALL command. Then you can manually remove the files comprising your Liberty profile application-serving environment.

## Before you begin

After installing the Liberty application-serving environment by executing a JAR file on IBM i, you might have used the iAdmin POSTINSTALL command to configure the Liberty server to launch as a job in the QWAS85 subsystem and to run under the QEJBSVR user profile. If so, you must remove the IBM i native objects and libraries created at that time before you manually remove the files that comprise your Liberty profile application-serving environment.

**Note:** You must have \*ALLOBJ and \*SECADM special authority to use the iAdmin POSTINSTALL command.

## Procedure

1. On the IBM i command line, run the STRQSH command to start the Qshell.
2. In the resulting Qshell session, change the directory to the wlp directory.
3. Run the following command.

```
lib/native/os400/bin/iAdmin PREUNINSTALL
```

## What to do next

Manually remove the files that comprise your Liberty profile application-serving environment.

---

## Installing Liberty Repository assets



8.5.5.2

You can use a variety of tools to install the assets that are in the Liberty Repository or download them directly from the WASdev website.

## Before you begin

**Important:** Product documentation that is marked with the  icon indicates information about assets that are available only from the Liberty Repository.

The Liberty Repository provides an online mechanism to deliver Liberty and additional content, enabling a single point of access for various asset types. For more information, see “Liberty: Liberty Repository” on page 965.

### Note:

- To install assets from the Liberty Repository, you must have Liberty for WebSphere Application Server Version 8.5.5.2 or later.
- To access the IBM WebSphere Liberty Repository with limited internet access or through a firewall, ensure that you have access to the following hosts and ports:
  - public.dhe.ibm.com on port 443
  - asset-websphere.ibm.com on port 443

## About this task

You can use several methods to access and install Liberty Repository assets. Some methods, such as Installation Manager, require the completion of specific steps in the installation sequence before you can install the applicable assets.

### Procedure

- Review the list of available assets in the Liberty Repository. See the Downloads page on WASdev.net. You can sort assets by date, name, or rating, or you can filter assets by asset type or Liberty edition. For a list of Liberty features, see “Liberty features” on page 826
- Review the installation methods for the Liberty Repository assets. Use the following table to determine the appropriate installation methods for each asset type:

Table 100. Installation methods for Liberty Repository asset types

Asset type	installUtility command	featureManager command	configUtility command	Installation Manager	Developer tools <sup>a</sup>	WASdev site <sup>b</sup>
Addons	✓	✓		✓	✓	✓
Admin scripts					✓	
Config snippets			✓		✓	✓
Features	✓	✓		✓	✓	
Open source integrations	✓			✓	✓	✓
Products				✓ <sup>c</sup>	✓	✓
Product samples	✓			✓	✓	✓
Tools						✓

**Note:**

- Developer tools are available only for the Linux, Mac OS, and Windows platforms.
- You can download assets from the WASdev.net website to install separately.
- You can install product runtimes from Installation Manager, but they are not in the Liberty Repository.

- Choose the installation method for the Liberty Repository assets that fits your usage scenario.
  - 8.5.5.6 installUtility** command: Finds, obtains information about, and installs a variety of assets that are in a local directory-based repository, an instance of the Liberty Asset Repository Service, or the IBM WebSphere Liberty Repository. You can also download Liberty Repository assets to your local system for offline use. The **installUtility** command downloads and installs all dependencies for the asset. For more information, see “Installing assets using the installUtility command” on page 1393.
  - featureManager** command: Installs Liberty Repository features and addons to an existing installation of Liberty or downloads them to your local system for offline use. For more information, see “Installing assets using the featureManager command” on page 1403. For Version 8.5.5.6 and later, use the **installUtility** command instead because it enables you to work with more asset types and from multiple repositories.
  - 8.5.5.5 configUtility** command: Downloads config snippet assets and enables you to replace configuration snippet variables with your input values. For more information, see “Downloading and customizing configuration snippets from the command line” on page 1577.
  - IBM Installation Manager: Installs Liberty Repository assets during the installation or an upgrade to a new version of Liberty. You can use the Installation Manager graphical user interface, command-line interface, or the Installation Manager in silent mode with a response file. For more information, see “Installing assets using Installation Manager” on page 1411.

- **Distributed operating systems** Developer tools: Developer tools for WebSphere Application Server, such as WebSphere Developer Tools, provide a graphical user interface that you can use to install Liberty Repository assets. For more information, see “Installing assets by using developer tools” on page 1413.
- WASdev site: You can download a subset of the Liberty Repository assets directly from the WASdev site. See the installation instructions for each downloadable asset on WASdev.net.

## Installing assets using the `installUtility` command



8.5.5.6

You can use the `installUtility` command to install assets in your Liberty environment and view required asset information.

### About this task

After you install Liberty, you can install assets by running the `installUtility` command. The `installUtility` command automatically installs asset dependencies.

You can install assets from the following repositories:

- The IBM WebSphere Liberty Repository, a public IBM-hosted repository that is accessible through the internet. For more information, see “Liberty: Liberty Repository” on page 965.
- The Liberty Asset Repository Service, an open-source service that you can use to create an on-premises repository that is remotely accessible behind the firewall of an enterprise. For more information, see the WASdev/tool.lars project on GitHub.
- Local directory-based repositories that are created by using the `installUtility download` action. For more information, see “Downloading assets using the `installUtility` command” on page 1400.

By default, the `installUtility` command is configured to install assets only from the Liberty Repository. If you want to install assets from a local directory-based repository or an instance of the Liberty Asset Repository Service, you must configure these repositories in the `repositories.properties` file. For more information, see “Configuring repositories and proxy settings for the `installUtility` command” on page 1401.

For a list of the actions and options for the `installUtility` command, see “Liberty: `installUtility` command” on page 1394.

### Procedure

1. Review the available assets and obtain the `shortName` for each asset that you want to install. You can use the `installUtility` command to search for and review assets, or you can find them on the Downloads page on WASdev.net.
  - To review assets and obtain the asset `shortName` by using the `installUtility` command, use the `installUtility find` command.
    - To find assets that are applicable to your configuration, use the `searchString` option. The following example searches for all assets that match the search string `jca`:
 

```
installUtility find jca
```
    - To find a specific type of asset, use the `--type=[feature|sample|opensource|addon|all*]` option. The following example searches for features that match the search string `jca`:
 

```
installUtility find jca --type=feature
```
  - To review assets and obtain the asset `shortName` from the WASdev website, see the asset details page on the WASdev website for each feature that you want to install. The `shortName` is found in the installation instructions of the asset details page; for example: the Portlet Container `shortName` is `portlet-2.0`.

For a list of all Liberty features, see “Liberty features” on page 826.

2. Run the **installUtility install** command to install the assets.

For example, the following command installs the `jca-1.6` feature:

```
installUtility install jca-1.6
```

To install multiple assets, separate each *shortName* with a space. For example, the following command installs both the `jca-1.6` feature and the `adminCenter-1.0` feature:

```
installUtility install jca-1.6 adminCenter-1.0
```

**Tip:** To install all features that apply your edition, you can install a feature bundle addon.

For example, to install all features for WebSphere Application Server Network Deployment Liberty, install the `ndControllerBundle` addon on servers that manage Liberty collectives and the `ndMemberBundle` addon on servers that are clustered and auto-scaled in a Liberty collective.

```
installUtility install ndControllerBundle
```

**z/OS** To install all features for WebSphere Application Server for z/OS Liberty, install the `zosBundle` addon.

```
installUtility install zosBundle
```

For a list of available addons, see Addon downloads on WASdev.

## Liberty: installUtility command

8.5.5.6

Use the **installUtility** command to find, obtain information about, and install assets that are in a directory-based repository, an instance of the Liberty Asset Repository Service, or the IBM WebSphere Liberty Repository.

### Asset sources

The **installUtility** command can access assets in the following repositories:

- The IBM WebSphere Liberty Repository, a public IBM-hosted repository that is accessible through the internet. For more information, see “Liberty: Liberty Repository” on page 965.
- The Liberty Asset Repository Service, an open-source service that you can use to create an on-premises repository that is remotely accessible behind the firewall of an enterprise. For more information, see the WASdev/tool.lars project on GitHub.
- Local directory-based repositories that are created by using the **installUtility download** action. For more information, see “Downloading assets using the installUtility command” on page 1400.

**8.5.5.8** You can use the **installUtility** command to work with directory-based repository assets directly from compressed repositories, such as `wlp-featureRepo-<version>.zip`, without extracting the archives. For more information about the `wlp-featureRepo-<version>.zip` file, see “Downloading assets using the installUtility command” on page 1400.

### Syntax

The command syntax is as follows:

```
installUtility action [options]
```

The *action* variable can take one of the following values:

#### download

Download assets from the repositories.

**find** Find assets in the repositories that are applicable to your configuration, or view detailed information about assets.

**install** Install assets or an enterprise subsystem archive (ESA) file to the run time, or deploy a server package and install the required features of the package.

**testConnection**

Test the repository connection.

**uninstall**

Uninstall features by specifying either the feature short name or the feature symbolic name. You can specify multiple features, separated by a space.

**Note:** Ensure that all server processes are stopped before you uninstall a feature.

**viewSettings**

View a template for configuring repositories or a proxy, or view the settings for the configured repositories or proxy.

**8.5.5.7** For Version 8.5.5.7 and later, this action also validates the settings for any configured repositories or proxy in the `repositories.properties` file.

**help** Display help information for a specified action.

## Options

The following options are available for the **installUtility download** command:

**--acceptLicense**

Accepts the license agreement.

**--viewLicenseAgreement**

View the license agreement.

**--viewLicenseInfo**

View the license agreement.

**--location=*directoryPath***

Specify the destination directory for the downloaded assets. This option is required.

**--overwrite**

Use this option to overwrite the existing files when you download assets to the local directory. The default behavior without the option is to ignore all the existing files.

**--verbose**

Use this option to display additional information during the download.

**name** Specify asset IDs to download one or more of the following assets, separating multiple asset IDs with a space:

- Features
- Addons
- Open source integrations
- Samples

The following options are available for the **installUtility find** command:

**8.5.5.7** **--from**

Specify a single directory-based repository as the source of the assets for the **installUtility** command.

**8.5.5.8** The directory-based repository can be an uncompressed folder or a compressed archive file, such as `wlp-featureRepo-<version>.zip`.

To search for assets in multiple directory-based repositories, you must configure the repositories in the `repositories.properties` file. For more information, see “Configuring repositories and proxy settings for the `installUtility` command” on page 1401.

**--showDescriptions**

Displays the description for each of the features that are found by the search.

**--type=[feature | sample | opensource | addon | all\*]**

Searches for the specified type of assets.

**--name**

Searches the asset name for the specified *searchString*.

**--verbose**

Use this option to display any available additional information while the action runs.

**searchString**

Finds assets that are applicable to your configuration. If you do not specify a search string, the command searches for all applicable assets.

The following options are available for the **installUtility install** command:

**--to=install\_option**

The `install_option` option can take one of the following values:

- `usr`: The feature is installed as a user feature. This value is the default value.
- `extension`: The location to install the feature. You can install the feature to any configured product extension location.

8.5.5.7

**--from**

Specify a single directory-based repository as the source of the assets for the **installUtility** command.

8.5.5.8

The directory-based repository can be an uncompressed folder or a compressed archive file, such as `wlp-featureRepo-<version>.zip`.

To install assets from multiple directory-based repositories, you must configure the repositories in the `repositories.properties` file. For more information, see “Configuring repositories and proxy settings for the `installUtility` command” on page 1401.

**--acceptLicense**

Indicate acceptance of license terms and conditions.

**--viewLicenseAgreement**

View the license agreement.

**--viewLicenseInfo**

View the license information.

**--verbose**

Use this option to display any available additional information while the action runs.

**name** Specify one or more assets that you want to install. You can specify the assets in the following ways:

**Asset IDs**

You can specify asset IDs to install one or more of the following assets, separating multiple asset IDs with a space:

- Features
- Addons
- Open source integrations
- Samples

### Server name

You can install features based on an existing server in the same Liberty environment by specifying the server name. The command installs any applicable features that are defined in the `server.xml` file of that server that are not already installed in the Liberty environment.

### Server package

You can specify a server package that you created by using the `server package --include=usr` command. The server package deploys, and the required features, which are defined in the `server.xml` file, are installed from the repositories.

#### 8.5.5.7 `server.xml` file

To install features based on a server configuration file, you can specify a path to any local `server.xml` file, such as `C:\localDir\server.xml`. The command installs any applicable features that are defined in the `server.xml` file that are not already installed in the Liberty environment.

### .esa file

Install a feature from an `.esa` file on your local file system. This action uses the `OSGI-INF/SUBSYSTEM.MF` manifest file from the `.esa` file as a new feature manifest. The manifest file specifies the name, contents, and dependencies of a feature. If you specify the `--to` option, `installUtility` copies the manifest file into the `${wlp.user.dir}/extensions/lib/features` directory, or the product extension directory. All of the bundles for the subsystem are extracted into the `${wlp.user.dir}/extensions/lib` directory and renamed as `{bundle symbolic name}_{bundle version}.jar`. License files, checksum files, globalization files, and other subsystem content are extracted to the location defined in the subsystem manifest.

The following option is available for the `installUtility testConnection` command:

#### *repoName*

Specifies the name of the repository to be tested. If not specified, all repositories that are specified in the `repositories.properties` file are tested.

The following option is available for the `installUtility uninstall` command:

#### 8.5.5.8 `--force`

Uninstall the specified feature regardless of whether other installed features have dependencies on it.

**Note:** Uninstalling a feature that is required by other installed features might cause those features to stop working and might prevent servers from running correctly.

#### `--noPrompts`

Uninstalls the feature without prompts. The default is false.

#### `--verbose`

Use this option to display additional information during the uninstallation.

*name* Specify one or more features to uninstall, separating multiple names with a space. You can specify the following options:

- The short name of the subsystem archive (ESA file), such as `adminCenter-1.0`.
- The symbolic name of the subsystem archive (ESA file), such as `com.ibm.websphere.appserver.adminCenter-1.0`.

8.5.5.8 You can uninstall user features and product extensions by prefixing the feature name with the extension followed by a colon, such as `usr:webCacheMonitor-1.0`.

8.5.5.7 The following option is available for the `installUtility viewSettings` command:

## --viewValidationMessages

Use this option to display the detailed messages from the validation of the configured repositories.properties file. Each message contains an error code, the line number where the error was found, and the cause of the error.

## Usage examples

Use the following example to display help information for the **install** action:

```
installUtility help install
```

Use the following example to install a user feature:

```
installUtility install my_feature --to=usr
```

Use the following example to install a user feature to the *my\_extension* product extension location:

```
installUtility install my_feature --to=my_extension
```

Use the following example to install multiple features:

```
installUtility install feature1 feature2 feature3
```

Use the following example to install a sample:

```
installUtility install mongoDBSample
```

**8.5.5.7** Use the following example to install a feature bundle add-on from a single local directory-based repository:

```
installUtility install ndMemberBundle --from=c:\download\wlp-featureRepo-8.5.5.7
```

**8.5.5.8** Use the following example to install a feature bundle add-on from a single compressed directory-based repository archive:

```
installUtility install ndMemberBundle --from=c:\download\wlp-featureRepo-8.5.5.8.zip
```

Use the following example to install a server:

```
installUtility install myServer
```

Use the following example to install a server package compressed .jar file:

```
installUtility install c:\temp\myServer.jar
```

Use the following example to install a local .esa file:

```
installUtility install c:\temp\myFeature.esa
```

Use the following example to install a server package compressed file:

```
installUtility install c:\temp\myServer.zip
```

Use the following example to find assets that are applicable to your configuration:

```
installUtility find searchString
```

Use the following example to find samples that are applicable to your configuration:

```
installUtility find searchString --type=sample
```

Use the following example to find a particular feature that is applicable to your configuration:

```
installUtility find webCacheMonitor-1.0 --name --type=feature
```

Use the following example to list detailed information:

```
installUtility find searchString --showDescriptions
```

Use the following example to download required dependencies from the repositories to a local directory:  
`installUtility download feature_shortName --location=c:\temp\download --acceptLicense`

Use the following example to test the connection to the Liberty Repository:

```
installUtility testConnection default
```

Use the following example to uninstall a feature:

```
installUtility uninstall adminCenter-1.0
```

**8.5.5.8** Use the following example to uninstall a user feature or product extension:

```
installUtility uninstall usr:webCacheMonitor-1.0
```

Use the following example to uninstall multiple features:

```
installUtility uninstall feature1 feature2 feature3
```

Use the following example to uninstall multiple features without prompts:

```
installUtility uninstall --noPrompts feature1 feature2 feature3
```

## Return codes

Table 101. Return codes and explanations.

Return code	Explanation
0	The command successfully completed the requested operation.
20	One or more arguments are not valid.
21	A runtime exception occurred because of one or more of the following conditions: <ul style="list-style-type: none"> <li>A runtime exception occurred during the installation of the .esa subsystem archive file.</li> <li>A license is not accepted or acknowledged.</li> <li>The .esa subsystem archive file did not extract correctly.</li> </ul>
22	The feature to be installed exists.
23	The feature definition was not valid for one or more of the following reasons: <ul style="list-style-type: none"> <li>The feature does not have a valid manifest file.</li> <li>The version of the feature is not supported in this Liberty environment.</li> <li>The .zip or .jar file that contains the feature files does not exist.</li> </ul>
24	The .esa subsystem archive file is missing content.
25	A file to be installed exists.
26	The product is not a core product, and the product extension files cannot be found.
27	The product is not a core product, and the product extension is not defined in the <code>\${wlp.install.dir}/etc/extensions/<i>extension_name</i>.properties</code> file.
28	The manifest files for the feature in the product extension cannot be found.
29	The feature is not valid for the current product.
<b>8.5.5.7</b> 30	The repositories.properties file failed the validation.

Table 101. Return codes and explanations (continued).

Return code	Explanation
33	The connection to the repository failed.
34	The repository name is not found. The provided repository name does not exist in the configuration file.
35	The action was canceled by the user.

## Downloading assets using the `installUtility` command



8.5.5.6

You can use the `installUtility` command to download assets to your local file system.

### Before you begin

Before you can access the IBM WebSphere Liberty Repository using the `installUtility` command, you must install Liberty for WebSphere Application Server.

### About this task

After you install Liberty, you can download assets to your local file system by running the `installUtility` command. Assets can be downloaded to a new directory, which you can then use as a repository, or to an existing directory-based repository.

By default, the `installUtility` command is configured to download assets only from the public IBM WebSphere Liberty Repository. If you want to download assets from a local directory-based repository or an instance of the Liberty Asset Repository Service, you must configure these repositories in the `repositories.properties` file. For more information, see “Configuring repositories and proxy settings for the `installUtility` command” on page 1401.

For a list of the actions and options for the `installUtility` command, see “Liberty: `installUtility` command” on page 1394.

**Tip:** Rather than downloading individual assets, you can download a `wlp-featureRepo-<version>.zip` file from IBM Fix Central. The `.zip` file contains a directory-based repository of all features and add-ons for the particular fix pack of Liberty that you download from IBM Fix Central. Extract the archive file to populate a local directory-based repository or an instance of the Liberty Asset Repository Service with the feature and add-on ESA files. Assets that are not included in the `.zip` file must be downloaded by using the `installUtility` command.

**8.5.5.8** For Version 8.5.5.8 and later, you can use the `installUtility` command to work with repository assets directly from the `wlp-featureRepo-<version>.zip` file and other compressed directory-based repositories without extracting the archives.

### Procedure

1. Review the available assets and obtain the `shortName` for each asset that you want to download. You can use the `installUtility` command to search for and review assets, or you can find them on the Downloads page on WASdev.net.
  - To review assets and obtain the asset `shortName` using the `installUtility` command, use the `installUtility find` command.
    - To find assets that are applicable to your configuration, use the `searchString` option. The following example searches for all assets that match the search string `adminCenter`:
 

```
installUtility find adminCenter
```

- To find a specific type of asset, use the `--type=[feature|sample|opensource|addon|all*]` option. The following example searches for features that match the search string `adminCenter`:

```
installUtility find adminCenter --type=feature
```

- To review assets and obtain the asset *shortName* from the WASdev website, see the asset details page on the WASdev website for each feature that you want to install. The *shortName* is found in the installation instructions of the asset details page; for example: the Portlet Container **shortName** is *portlet-2.0*.

2. Run the **installUtility download** command to download the assets. You must specify a target directory for the downloaded assets on the `--location` option.

For example, the following command downloads the `adminCenter-1.0` feature to the `c:\temp\download` directory:

```
installUtility download adminCenter-1.0 --location=c:\temp\download
```

You can download multiple assets at once by separating each asset *shortName* with a space. For example, the following command downloads both the `jca-1.6` feature and the `adminCenter-1.0` to the `c:\temp\download` directory:

```
installUtility download jca-1.6 adminCenter-1.0 --location=c:\temp\download
```

## What to do next

After you download assets to your local file system, you can add a local directory to your repository configuration so that you can install assets from the directory. For more information about configuring repositories, see “Configuring repositories and proxy settings for the `installUtility` command.”

## Configuring repositories and proxy settings for the `installUtility` command

8.5.5.6

In the `repositories.properties` file, you can configure how the **installUtility** command accesses local directory-based repositories, instances of the Liberty Asset Repository Service, and the IBM WebSphere Liberty Repository.

### About this task

The **installUtility** command can access the following repositories:

- The IBM WebSphere Liberty Repository, a public IBM-hosted repository that is accessible through the internet. For more information, see “Liberty: Liberty Repository” on page 965.
- The Liberty Asset Repository Service, an open-source service that you can use to create an on-premises repository that is remotely accessible behind the firewall of an enterprise. For more information, see the WASdev/tool.lars project on GitHub.
- Local directory-based repositories that are created by using the **installUtility download** action. For more information, see “Downloading assets using the `installUtility` command” on page 1400.

Both the **installUtility** command and the **featureManager** command use the same configuration properties file, `repositories.properties`. The proxy settings are shared, but the repository settings are used only by the **installUtility** command. To manage assets and complete repository-based installation, find, or uninstallation operations, use the **installUtility** command instead of the **featureManager** command.

**Tip:** You can download or install assets from a single local directory-based repository by specifying the repository on the `--from` option. No additional configuration in the `repositories.properties` file is required. For more information, see “Liberty: `installUtility` command” on page 1394.

To access the IBM WebSphere Liberty Repository with limited internet access or through a firewall, ensure that you have access to the following hosts and ports:

- `public.dhe.ibm.com` on port 443

- `asset-websphere.ibm.com` on port 443

**Note:** The `installUtility` command supports only proxy servers with HTTP/HTTPS protocols.

## Procedure

1. Optional: When you first configure the repository or proxy settings, you can run the `installUtility viewSettings` command to output a configuration template for the `repositories.properties` file.

Copy the template into a new properties file at `${wlp.install.dir}/etc/repositories.properties`. The properties file must be in ASCII format for all platforms.

2. Define the settings in the `${wlp.install.dir}/etc/repositories.properties` file.

If you copied the template from the `installUtility viewSettings` command, modify the template by changing the example repository and proxy settings to refer to your environment. Lines that begin with a number sign (#) are not processed.

- To disable access to the Liberty Repository, set the `useDefaultRepository` property to `false`. The Liberty Repository is enabled by default and is the last repository that is accessed when you install or download assets.

```
useDefaultRepository=false
```

- To define a repository, add a property as `repoName.url=url`. Each repository name must be unique.

The defined repositories are accessed in the order that they are specified in the `repositories.properties` file. For Version 8.5.5.7 and later, you can also specify `repoName.url=file_path`.

### Windows

```
dev-rep.url=http://dev.repo.ibm.com:9080/ma/v1
local-rep2.url=file:///c:/IBM/localrepo2
```

8.5.5.7

`local-rep3.url=C:\IBM\localrepo3`

8.5.5.8

`local-rep4.url=C:\IBM\localrepo4.zip`

HP-UX

Solaris

Linux

UNIX

z/OS

```
dev-rep.url=http://dev.repo.ibm.com:9080/ma/v1
local-rep2.url=file:///usr/IBM/localrepo2
```

8.5.5.7

`local-rep3.url=/usr/IBM/localrepo3`

8.5.5.8

`local-rep4.url=/usr/IBM/localrepo4.zip`

- If a repository requires a user name and password, set the properties `repoName.user=userId` and `repoName.userPassword=password`.

If a user name and password are required and they are not set, you receive a prompt to provide them. For enhanced security, encode the password by using the `securityUtility encode` action; for more information, see Liberty `securityUtility` command. For Version 8.5.5.6, the password must be encoded to connect to the repository.

```
dev-rep.user=myname
dev-rep.userPassword={aes}AH5NLyd7DfGb12pK17Pw+
```

- If your system requires access to the IBM WebSphere Liberty Repository or an instance of the Liberty Asset Repository Service through a proxy server, set the `proxyHost`, `proxyPort`, `proxyUser`, and `proxyPassword` proxy properties.

For enhanced security, encode the value of the `proxyPassword` property by using the `securityUtility encode` action. If you do not set the user name and password, you receive a prompt to provide them. For Version 8.5.5.6, the password must be encoded to connect to the proxy.

For example:

```
proxyHost=my.proxy.server.ibm.com
proxyPort=9080
proxyUser=myname
proxyPassword={aes}AH5NLyd7DfGb12pK17Pw+
```

3. Save the changes to the `repositories.properties` file.
4. Review the repository and proxy settings by running the `installUtility viewSettings` command.

**8.5.5.7** When you run the **installUtility viewSettings** command, the repository and proxy configuration is automatically validated. To view detailed validation messages, run the command with the **--viewValidationMessages** option. **8.5.5.7**

```
>installUtility viewSettings
```

```
installUtility Settings
```

```
-----  
Properties File: c:\wlp\etc\repositories.properties  
Default Assets Repository: IBM WebSphere Liberty Repository  
Use Default Repository: True
```

```
Properties File Validation
```

```
-----  
Validation Results: The properties file successfully passed the  
validation.
```

```
Configured Repositories
```

```
-----  
Name: dev-rep  
Location: http://dev.repo.ibm.com:9080/ma/v1  
User Name: myname  
Password: <Unspecified>
```

```
Proxy Settings
```

```
-----  
Proxy Server: my.proxy.server.ibm.com  
Port: 9080  
User Name: myname  
Password: *****
```

5. Test the repository connection by running the **installUtility testConnection** command. If you do not set the user name and password, you receive a prompt to provide them. Use the following example to test the repository connection:

```
>installUtility testConnection  
Testing the connection to all configured repositories...  
This process might take several minutes to complete.
```

```
Configured Repositories
```

```
-----  
Name: dev-rep  
Location: http://dev.repo.ibm.com:9080/ma/v1  
Status: Successfully connected to the configured repository.
```

You can test all configured repositories in the `repositories.properties` file at once by running the **installUtility testConnection** command with no `repoName` specified. The repository name for the Liberty Repository is *default*. To test the connection to the Liberty Repository, run the following command:

```
installUtility testConnection default
```

## What to do next

You can use the **installUtility** command to search for assets and install or download them from the configured repositories.

## Installing assets using the `featureManager` command



**8.5.5.2**

You can use the **featureManager** command to install Liberty Repository features in your Liberty environment.

## Before you begin

Before you can access the Liberty Repository using the **featureManager** command, you must install Liberty for WebSphere Application Server Version 8.5.5.2 or later.

## About this task

After you install Liberty, you can install Liberty Repository features by running the **featureManager** command. The **featureManager** command automatically installs asset dependencies.

**Tip:**  Use the **installUtility** command instead of the **featureManager** command. With the **installUtility** command, you can manage more asset types and install, find, or download assets from multiple repositories. For more information, see “Installing assets using the installUtility command” on page 1393.

## Procedure

-  Review the assets that are located in the Liberty Repository and obtain the *feature\_shortName* for each asset that you want to install. The asset *feature\_shortName* is required to download and install assets. You can use the **featureManager** command to search for and review assets, or you can find them on the Downloads page on WASdev.net.
  - To review assets and obtain the asset *feature\_shortName* using the **featureManager** command, use the **featureManager find** command.
    - To find assets that are applicable to your configuration, specify a string to search for:  
`featureManager find searchString`
    - To view detailed information, use the **--viewInfo** option; for example:  
`featureManager find searchString --viewInfo`
  - To review assets and obtain the asset *feature\_shortName* from the WASdev website, see the asset details page on the WASdev website for each feature that you want to install. The *feature\_shortName* is found in the installation instructions of the asset details page; for example: the Portlet Container *feature\_shortName* is *portlet-2.0*.

For a list of all Liberty features, see “Liberty features” on page 826.

- Obtain the *feature\_shortName* from the asset details page on the WASdev website for each feature that you want to install. The *feature\_shortName* is found in the installation instructions of the asset details page; for example: the Portlet Container *feature\_shortName* is *portlet-2.0*.
- Run the **featureManager** command to install the assets. Run the following command:

```
bin/featureManager install feature_shortName --when-file-exists=ignore
```

To install multiple features, use spaces or commas to separate each *feature\_shortName*; for example:

```
bin/featureManager install feature_shortName1 feature_shortName2 --when-file-exists=ignore
```

 To download a feature to a local directory without installing the feature, use the **--downloadOnly** option; for example:

```
bin/featureManager install feature_shortName1 feature_shortName2 --downloadOnly=[all|required*|none]
```

You can configure this option to download all the dependent features, the dependent features required for this runtime, or none of the dependent features. The default is to download the required dependent features. To specify a local destination directory, use this option with the **--location=directoryPath** option.

 To install features from a local source directory, use the **--location=directoryPath** option; for example:

```
bin/featureManager install feature_shortName1 feature_shortName2 --location=directoryPath
```

**Note:** **z/OS** **8.5.5.4** Beginning with Version 8.5.5.4, the SMP/E-managed repository for WebSphere Application Server for z/OS Version 8.5 includes a complete set of Liberty features at the current fix pack level. You can access these with the **featureManager** command by specifying the following command:

```
--location=/usr/lpp/InstallationManagerRepository/HBB0850/WLP/fixpacks/<fix pack level>/files
```

For example:

```
--location=/usr/lpp/InstallationManagerRepository/HBB0850/WLP/fixpacks/8.5.5.4/files
```

**8.5.5.8** As of Version 8.5.5.8, the Liberty features in this repository are stored in the format that is required by the **installUtility** command and can no longer be installed with the **featureManager** command. Use the **installUtility** command to install the features. For more information, see “Installing assets using the installUtility command” on page 1393.

 **8.5.5.4** If you do not want to connect to the Liberty Repository, use the **--offlineOnly** option to install features from a local directory; for example:

```
bin/featureManager install feature_shortName1 feature_shortName2 --offlineOnly --location=directoryPath
```

4. Use the **featureManager** command to see what assets you have installed or to get help. For more information, see: “Liberty:featureManager command”

## Liberty:featureManager command

### 8.5.5.0

You can use the **featureManager** command to find, install, uninstall, or obtain details about features.

The feature that you want to install must be packaged as a subsystem archive (ESA file).

**8.5.5.5** You can access the Liberty Repository using the **featureManager** command through a proxy server. For more information, see “Configuring proxy server support for the featureManager command in Liberty” on page 1410.

**Tip:** **8.5.5.6** Use the **installUtility** command instead of the **featureManager** command. With the **installUtility** command, you can manage more asset types and install, find, or download assets from multiple repositories. For more information, see “Installing assets using the installUtility command” on page 1393.

## Syntax

The command syntax is as follows:

```
featureManager action [options]
```

where *action* can take one of the following values:

**install** Install a feature from an enterprise subsystem archive (ESA) file, a URL to an ESA file, a feature short name, or a feature symbolic name.

If you specify a feature short name or a symbolic name, the feature is downloaded from an online repository hosted by IBM.

The *install* action uses the OSGI-INF/SUBSYSTEM.MF file from the ESA file as a new feature manifest that can be copied into the `/${wlp.user.dir}/extensions/lib/features` directory (or product extension directory if a value is specified for the **--to** property) being renamed after the symbolic name of the subsystem. All of the bundles for the subsystem will be extracted into the `/${wlp.user.dir}/extensions/lib` directory and renamed as `{bundle symbolic name}_{bundle version}.jar`. License files, checksum files, localization files and other subsystem content will also be extracted to the location defined in the subsystem manifest.



### 8.5.5.2

The **featureManager** command can download assets from the Liberty Repository; for more information, see “Installing Liberty Repository assets” on page 1391.

#### 8.5.5.5

### **uninstall**

Uninstall features using either the feature short name or the feature symbolic name.

#### **Note:**

- Ensure that all server processes are stopped before you uninstall a feature.
- The **uninstall** command cannot uninstall user features; for example: `webCacheMonitor-1.0`.

### **featureList**

Generate an XML file that contains a report that details all the features that are installed.



#### 8.5.5.4

### **find**

Find assets in the Liberty Repository that are applicable to your configuration.

#### 8.5.5.4

### **classpath**

Generate a JAR file that can be added to a compiler classpath in order to use APIs from a list of features. This action enables you to compile build scripts against the API JARs that are included in the product without referencing specific JAR names, which can change when a fixpack is applied. The output JAR contains relative paths to the API JARs in the product. Therefore, you must not move the output JAR to another directory.

**Note:** The **--features** option must be specified with this action.

**help** Display help information for a specified action.

## **Options**

The following options are available for the **featureManager install** command:

### **--acceptLicense**

Automatically indicate acceptance of license terms and conditions.

#### 8.5.5.4

### **--downloadOnly=[all | required\* | none]**

Download the requested feature to a local directory without installing the feature. This option can be configured to download all the dependent features, the dependent features required for this runtime, or none of the dependent features. The default is to download the required dependent features. Specify the directory with the **--location** option.

**Note:** You cannot use this option if you specify the subsystem archive location with a file name or URL.

#### 8.5.5.4

### **--location=directoryPath**

Specifies the location of the subsystem archive that you want to install. When used with the **--downloadOnly** option, this option specifies a destination directory for downloaded features. This option is required when using the **--downloadOnly** and **--offlineOnly** options.

**Note:** You cannot use this option if you specify the subsystem archive location with a file name or URL.

#### 8.5.5.4

### **--offlineOnly**

Use this option if you do not want to connect to the Liberty Repository. Instead, the command only installs features from the local directory. The local directory is specified with the **--location** option.

**Note:** You cannot use this option if you specify the subsystem archive location with a file name or URL.

**--to=*install\_option***

where *install\_option* can take one of the following values:

- **usr**: The feature is installed as a user feature. This is the default value.
- **extension**: The location to which you want to install the feature. You can install the feature to any configured product extension location.

**--viewLicenseAgreement**

View license agreement.

**--viewLicenseInfo**

View license information.

**--when-file-exists=*exist\_option***

Specifies the action to take if a file to be installed already exists. *exist\_option* can take one of the following values:

- **fail**: Cancel the installation.
- **ignore**: Continue the installation and ignore the file that exists.
- **replace**: Overwrite the existing file.

**--verbose**

Use this option to display any available additional information while the action runs.

***subsystem\_archive***

Specifies the location of the subsystem archive that you want to install. You can specify the location in the following ways:

- A file name; for example: `my_feature.esa`.
- A URL, for example:

`http://myhost.ibm.com/liberty/assets/my_feature.esa`

- **8.5.5.2** The short name of the subsystem archive (ESA file), such as `adminCenter-1.0`
- **8.5.5.2** The symbolic name of the subsystem archive (ESA file), such as `com.ibm.websphere.appserver.adminCenter-1.0`

For more information, see the Downloads page on WASdev.net.

**Note:** Specify multiple features by separating the features with a comma or a space. For versions prior to Version 8.5.5.7, multiple features must be separated by a comma.

**8.5.5.5** The following options are available for the **featureManager uninstall** command:

**8.5.5.8** **--force**

Uninstall the specified feature regardless of whether other installed features have dependencies on it.

**Note:** Uninstalling a feature that is required by other installed features might cause those features to stop working and might prevent servers from running correctly.

**--noPrompts**

Uninstall features without any user interaction or confirmation messages.

**--verbose**

Use this option to display any available additional information while the action runs.

***name*** Specify the feature to uninstall. You can specify the following options:

- The short name of the subsystem archive (ESA file), such as `adminCenter-1.0`.
- The symbolic name of the subsystem archive (ESA file), such as `com.ibm.websphere.appserver.adminCenter-1.0`.

**Note:** Specify multiple features by separating the features with a comma or a space. For versions prior to Version 8.5.5.7, multiple features must be separated by a comma.

The following options are available for the **featureManager featureList** command:

**--encoding=*charset***

where *charset* is the character set to use when creating the XML report file.

**--locale=*language***

where *language* specifies the language to use when creating the XML report file. This consists of the ISO-639 two-letter lowercase language code, optionally followed by an underscore and the ISO-3166 uppercase two-letter country code.

**--productExtension=*name***

where *name* is the product extension name whose features are to be listed. If the product extension is installed in the default user location, use the keyword: `usr`. If this option is not specified, the action is taken on WebSphere Application Server Liberty Core.

**XML\_report\_file\_name**

Specifies the name of the XML report file that you want to create.

The following options are available for the **featureManager find** command:

**8.5.5.4 --viewInfo**

View detailed information.

**--verbose**

Use this option to display any available additional information while the action runs.

**8.5.5.4 searchString**

Use the *searchstring* option to find applicable features from the IBM WebSphere Liberty Repository

**8.5.5.4** The following options are available for the **featureManager classpath** command:

**--features=*feature1,feature2,...***

The list of features that contain the list of API JAR files. This option is required for the classpath action.

**fileName**

The name of the generated JAR file.

## Usage examples

The following example installs the subsystem archive `my_feature.esa` as a user feature:

```
featureManager install my_feature.esa --to=usr
```

The following example installs the subsystem archive `my_feature.esa` to the `my_extension` product extension location:

```
featureManager install my_feature.esa --to=my_extension
```

The following example generates a report for all installed features; the report is written to the file `my_feature_report.xml` using the Brazilian Portuguese language:

```
featureManager featureList my_feature_report.xml --locale=pt_BR
```

The following example generates a report that contains all installed features that are defined in the product extension that is installed in the default user location `wlp/usr/extension`, which is known by the runtime environment as the `usr` product extension. The report is written to the file `my_feature_report.xml`:

```
featureManager featureList --productExtension=usr my_feature_report.xml
```

The following example generates a report that contains all features that are defined in the product extension that is installed in the location pointed to by the content in the *productExtensionName.properties* file in the product installation's *etc/extensions* directory. The report is written to the file *my\_feature\_report.xml*:

```
featureManager featureList --productExtension=productExtensionName my_feature_report.xml
```

The following example displays help information for the *install* action:

```
featureManager help install
```



8.5.5.4

The following example finds applicable assets from the Liberty Repository:

```
featureManager find searchString
```



8.5.5.4

The following example lists detailed information:

```
featureManager find searchString --viewInfo
```



8.5.5.4

The following example downloads required dependencies from the Liberty Repository to a local directory and does not install them:

```
featureManager install feature_shortName --downloadOnly --location=c:\temp\download --acceptLicense
```

**Note:** You cannot use this option if you specify the subsystem archive location with a URL.



8.5.5.4

The following example downloads all dependencies from the Liberty Repository and does not install them:

```
featureManager install feature_shortName --downloadOnly=all --location=c:\temp\download --acceptLicense
```

**Note:** You cannot use this option if you specify the subsystem archive location with a URL.



8.5.5.4

The following example installs features that are located in a local directory. If there are missing dependencies, they are installed from the online repository:

```
featureManager install feature_shortName --location=c:\temp\download --acceptLicense
```

**Note:** You cannot use this option if you specify the subsystem archive location with a URL.



8.5.5.4

The following example installs assets from a local directory without downloading missing dependencies from the Liberty Repository:

```
featureManager install feature_shortName --location=c:\temp\download --offlineOnly
```

**Note:** You cannot use this option if you specify the subsystem archive location with a URL.



8.5.5.4

The following example creates a classpath JAR file and compiles an application class that uses it:

```
featureManager classpath --features=servlet-3.0 classpath.jar  
javac -cp classpath.jar TestServlet.java
```



8.5.5.5

The following example uninstalls a feature:

```
featureManager uninstall adminCenter-1.0
```

## Return codes

Table 102. Return codes and explanations

Return code	Explanation
0	The command successfully completed the requested operation.
20	One or more arguments are not valid.
21	A runtime exception occurred because of one or more of the following conditions: <ul style="list-style-type: none"><li>• A runtime exception occurred while installing the .esa subsystem archive file.</li><li>• A license is not accepted or acknowledged.</li><li>• The .esa subsystem archive file did not extract correctly.</li></ul>
22	The feature that you wanted to install already exists.
23	The feature definition was not valid for one or more of the following reasons: <ul style="list-style-type: none"><li>• The feature does not have a valid manifest file.</li><li>• The version of the feature is not supported in this Liberty environment.</li><li>• The .zip or .jar file that contains the feature files does not exist.</li></ul>
24	The .esa subsystem archive file is missing content.
25	A file that you wanted to install already exists, and you specified the <b>when-file-exists=fail</b> option.
26	The product is not a core product, and the product extension files cannot be found.
27	The product is not a core product, and the product extension is not defined in the <code>\${wlp.install.dir}/etc/extensions/<i>extension_name</i>.properties</code> file.
28	The manifest files for the feature in the product extension cannot be found.
29	The feature is not valid for the current product.

## Configuring proxy server support for the featureManager command in Liberty

8.5.5.5

You can access the Liberty Repository using a proxy server.

### Before you begin

Ensure that you have created the required directory structure. If the etc directory is not found in the Liberty installation directory, then you must create it.

### About this task

You can run the **featureManager** command to connect to the IBM WebSphere Liberty Repository through a user-specified proxy server.

#### Note:

- The **featureManager** command only supports proxy servers with HTTP/HTTPS protocols.

- The proxy server is only supported for the install and find options for the **featureManager** command.
- To access the IBM WebSphere Liberty Repository with limited internet access or through a firewall, ensure that you have access to the following hosts and ports:
  - public.dhe.ibm.com on port 443
  - asset-websphere.ibm.com on port 443

**8.5.5.6** Both the **featureManager** command and the **installUtility** command use the same configuration properties file, `repositories.properties`. The proxy settings are shared, but the repository settings are only used by the **installUtility** command. Using the **installUtility** command is recommended over the **featureManager** command because it enables you to work with more asset types and from multiple repositories; for more information see “Configuring repositories and proxy settings for the installUtility command” on page 1401.

To configure proxy server support for the **featureManager** command, complete the following steps.

### Procedure

1. In the `<Liberty_installation_dir>/etc` directory, create an ASCII properties file, and name it `repositories.properties`.
2. In the `repositories.properties` file, specify the following properties with the proxy server configurations:
  - a. Specify the proxy server host name with no protocol information.  
`proxyHost=proxy.xyz.com`
  - b. Specify the proxy server port number:  
`proxyPort=8080`
  - c. Specify the proxy server user name and encrypted password. The proxy server password must be encrypted by using the **securityUtility** command found in the `<Liberty_installation_dir>/bin/` directory.  
For more information about the encoding options, see: “Liberty:securityUtility command” on page 1844. If the proxy server does not require authentication, then the **proxyUser** and **proxyUserPassword** properties are not required.  
`proxyUser=user`  
`proxyUserPassword={aes}Ly0wJyYPKDs=`
3. Save the `repositories.properties` file.

### What to do next

Run the `featureManager install name` or `featureManager find searchString --viewInfo` commands to install or query applicable Liberty features from the IBM Liberty Repository through the specified proxy server. For more information, see “Liberty:featureManager command” on page 1405.

## Installing assets using Installation Manager



### 8.5.5.2

If you have IBM Installation Manager installed, you can download and install Liberty Repository assets when you install or upgrade Liberty.

### Before you begin

**Note:** To install Liberty Repository assets, you must have IBM Installation Manager Version 1.6.2 or later and be installing or upgrading to Liberty for WebSphere Application Server Version 8.5.5.2 or later.

## About this task

This task applies only to installing Liberty Repository features or add-ons during the installation or upgrade of Liberty for WebSphere Application Server Version 8.5.5.2 or later. For information about installing product samples and open source integrations, see Installation Manager repository for Liberty samples on WASdev.net. For a list of all assets and their descriptions, see the Downloads page on WASdev.net.

You can install Liberty Repository assets from the following repositories:

- The IBM WebSphere Liberty Repository, a public IBM-hosted repository that is accessible through the internet. For more information, see “Liberty: Liberty Repository” on page 965.
- **8.5.5.6** The Liberty Asset Repository Service, an open-source service that you can use to create an on-premises repository that is remotely accessible behind the firewall of an enterprise. For more information, see the WASdev/tool.lars project on GitHub.
- **8.5.5.6** Local directory-based repositories that are created by using the **installUtility download** action. For more information, see “Downloading assets using the installUtility command” on page 1400.

Rather than downloading individual assets, you can download a `wlp-featureRepo-<version>.zip` file from IBM Fix Central. The .zip file contains a directory-based repository of all features and add-ons for that fix pack. Downloading assets using these methods creates a `repository.config` file in the repository that you must point to from Installation Manager.

You can add the directory-based and Liberty Asset Repository Service repositories to Installation Manager in the same manner that you add the product offering repositories, then install assets from the repositories. Assets are installed from the repositories in the order that you specify them. If these repositories do not contain the assets that you want to install, the assets are installed from the IBM WebSphere Liberty Repository unless you disable it.

To access the IBM WebSphere Liberty Repository with limited internet access or through a firewall, ensure that you have access to the following hosts and ports:

- `public.dhe.ibm.com` on port 443
- `asset-websphere.ibm.com` on port 443

## Procedure

1. **8.5.5.6** Optional: Set up an instance of the Liberty Asset Repository Service or a local directory-based repository, then specify the repository URL or directory path in Installation Manager.  
**8.5.5.8** For Version 8.5.5.8 and later, you can also specify the file path of a directory-based repository compressed in an archive file.
2. Install Liberty and Liberty Repository assets.
  - **Distributed operating systems** Choose from the following options for working with Installation Manager:
    - Graphical User Interface (GUI) - The Installation Manager GUI provides a list of available assets and detailed descriptions of each asset. See “Installing Liberty on distributed operating systems using the GUI” on page 1171.
    - Command line - The **imcl** command can download and install assets. See “Installing Liberty on distributed operating systems by using the command line” on page 1174.
    - Response files - Installation Manager supports installing assets using recorded or manually created response files. See “Installing Liberty on distributed operating systems by using response files” on page 1178.
  - **IBM i** Choose from the following options for working with Installation Manager:

- Command line - The **imcl** command can download and install assets. See “Installing Liberty on IBM i operating systems using the command line” on page 1294.
- Response files - Installation Manager supports installing assets using recorded or manually created response files. For detailed steps about installing assets using Installation Manager in silent mode, see “Installing Liberty on IBM i operating systems using response files” on page 1299.
- **z/OS** The **imcl** command can download and install assets. See “Installing WebSphere Application Server Liberty for z/OS” on page 1353.

## Installing assets by using developer tools

Distributed operating systems



8.5.5.2

If you have developer tools installed, you can install feature assets, open source integration assets, product sample assets, runtime assets, add-on assets, and config snippet assets from the Liberty Repository.

### About this task

Developer tools for WebSphere Application Server, such as IBM WebSphere Application Server Developer Tools for Eclipse, provide a graphical user interface that you can use to install Liberty Repository assets. This task shows you how to install assets by using WebSphere Developer Tools, Version 8.5.5.2 and later versions.

### Procedure

- Optional: Install assets from the Servers view.

If you create a Liberty server and a Liberty runtime environment, either from an archive or from the Liberty repository, you can install the following assets on the new runtime environment in the Servers view:

- Feature assets
- Open source integration assets
- Product runtime environment assets
- Product sample assets
- Add-on assets

You can install configuration snippet assets after you create a Liberty server. For more information, see “Creating a Liberty server by using developer tools” on page 1424.

- Install assets from the Runtime Explorer view.

In the Runtime Explorer view, you can install the following assets when you create a runtime environment or when you create a server in a runtime environment:

- Feature assets
- Open source integration assets
- Product sample assets
- Add-on assets

For more information, see the “Exploring the runtime environment by using developer tools” on page 1561 topic.

- Review the assets on the Downloads page on WASdev.net.

You can use search and filters to narrow your search results. Assets that you can install by using WebSphere Developer Tools are included on the site, along with assets that you can download by other methods.

## Adding more repositories by using developer tools

8.5.5.7

You can configure the list of repositories that are available for access by the tools. You can add remote repositories or local, directory-based repositories.

### Before you begin

- To create an on-premises repository that is remotely accessible behind the firewall of an enterprise, see the `WASdev/tool.lars` project on GitHub.
- To create a local, directory-based repository by using the `installUtility` download action, see `Downloading assets using the installUtility command`.

### Procedure

1. Open the Runtime Explorer view.
  - a. Select **Window > Show View > Other** from the workbench toolbar.
  - b. Select **Server > Runtime Explorer** in the Show View window.
2. Right-click the runtime environment, and then select **Install additional content...**.  
The Install Additional Content window is displayed.
3. Click **Configure Repositories**.  
The Configure Repositories window is displayed.
4. Add a repository.
  - a. To add a repository, click **Add...**
  - b. Enter a name for the repository in the **Name** field.
  - c. Enter the location for the repository.
    - To use a remote repository, select **Remote Repository**, and then enter the connection information.
    - To use a repository in a local directory, select **Local Repository**. Then, enter or browse to the location of the assets, which you downloaded by using the `installUtility` command of the runtime environment, or from the Liberty Repository.
    - **8.5.5.8** To use a repository in a .zip file, select **Browse**, and then browse to your .zip file. You can download a `wlp-featureRepo-<version>.zip` file from IBM Fix Central. The .zip file contains a directory-based repository of all features and add-ons for that fix pack.
  - d. Click **OK**.

### What to do next

In the Configure Repositories window, you can add, edit, remove, and reorder repositories.

The repository list is in descending order of priority. If an asset is contained in more than one repository, then the repository that is found first in the list is used during installation. Ensure that your repository is selected.

---

## Verifying the integrity of Liberty installation

8.5.0.1

You can use the command utilities to verify the installation integrity of Liberty.

## About this task

After you have installed Liberty, you must make sure that the installation is completed successfully and that all required features or iFixes are installed. The `productInfo` command provides different options to complete the following tasks:

- Compare the differences between APAR fixes and the current installation.
- Validate the MD5 checksum file for server installation and each feature.
- Verify the version information of the current installation.
- Verify the feature list on the current installation.

## Liberty:productInfo command

8.5.0.1

Use the **productInfo** command to validate the product integrity, compare different versions of the Liberty servers, and verify the current product versions.

### Syntax

The command syntax is as follows:

```
productInfo action --[options]
```

Where the possible values of the *options* vary depending on the value of the *action* parameter.

### Parameters

The following *action* parameters and *options* values are available for the **productInfo** command:

#### compare

Allows you to compare APAR fixes that are installed in the current installation with a different version of Liberty.

**--target**=*path to directory or archive file*

Specifies the target file with which to compare the current installation. The value of **--target** can be either a directory or an archive file that must be a valid Liberty installation location. This option is required if **--apars** is not specified.

**--apars**=*a comma separated list of APAR IDs*

Checks the current installation against this comma-separated list of APAR IDs to see if it contains them, and then lists any APARs that are not included. This option is required if **--target** is not specified.

**--output**=*path to an output file*

Outputs the result from this command to the supplied file name. By default, the output is directed to standard output.

**--verbose**

Displays detailed error messages when an error occurs.

**Note:** At least one of **--target** or **--apars** must be supplied

#### featureInfo

Lists all the features that are installed on the current Liberty server including any installed product extensions.

**--output**=*path to an output file*

Outputs the result from this command to the supplied file name. By default, the output is directed to standard output.

## validate

Validates the Liberty server.

**--output=***path to an output file*

Outputs the result from this command to the supplied file name. By default, the output is directed to standard output.

## version

Displays the product name and version.

The output includes the name and version of product extensions if a *product\_extension.properties* file is provided in the product extension installations versions directory containing the following properties:

`com.ibm.websphere.productVersion=your_product_version.`

`com.ibm.websphere.productName=your_product_name.`

**--output=***filename*

Outputs the result from this command to the supplied file name. By default, the output is directed to standard output.

**--verbose**

Displays the whole content of each properties file.

**--ifixes**

Displays the APAR fixes that are applied to the system, and the interim fixes that applied them.

For more information, refer to “Provide product information for your feature extension” on page 1823

### 8.5.5.6 viewLicenseAgreement

Displays the license agreement for the Liberty edition that is installed.

### 8.5.5.6 viewLicenseInfo

Displays the license information for the Liberty edition that is installed.

**help** Displays help information for the specific action.

## Usage

The following examples demonstrate correct syntax: 8.5.5.6

```
productInfo compare --target=C:\wlp\newInstall\wlp
productInfo compare --target=C:\wlp\newInstall.jar --output=C:\wlp\compareOutput.txt
productInfo compare --apars=com.ibm.ws.apar.PM39074,com.ibm.ws.apar.PM39075,com.ibm.ws.apar.PM39080
productInfo featureInfo --output=c:\wlp\featureListOutput.txt
productInfo validate
productInfo help compare
productInfo version
productInfo viewLicenseAgreement
productInfo viewLicenseInfo
```

---

## Docker support in Liberty

### 8.5.5.5

Docker is an open source platform that uses Linux containerization and a layered file system. The image that is built by using Docker consists of layers that contain the application and the dependent binary files and libraries, but uses the kernel from the host operating system. The layering allows changes to be made quickly because only the modified layers are rebuilt and deployed.

Liberty is designed to run in a container on multiple platforms compatible with the Docker engine. Specifically, Liberty has been tested on IBM Containers, Docker Datacenter, and OpenShift V3. To qualify for support, the base operating system that is used within the container must be a platform supported by the Liberty product.

For more information about Docker and its advantages, see [What is Docker?](#)

Docker Hub is a public repository that hosts Docker images. A Docker image for WebSphere Application Server for Developers Liberty is available on Docker Hub along with the documentation that describes its usage.

Running Liberty under Docker is also supported for production usage. Instructions and Dockerfiles for building production licensed Docker images by using the installation files that are obtained from Passport Advantage can be found on WASdev GitHub.

---

## Accessing a remote Liberty server in a Docker container by using developer tools

8.5.5.8

You can set up your remote Liberty server in a Docker container so that you can access it by using WebSphere Developer Tools. After you complete this setup, you can use WebSphere Developer Tools to configure and start your remote Liberty server.

### Before you begin

1. Install Docker, Cloud Foundry Command Line Interface (CLI), and the Cloud Foundry plug-in for IBM Containers.

For more information about installation, see [IBM Containers plug-in](#).

2. Log in to your Bluemix account, choose your organization and space, and then log in to your IBM Containers service.

For more information about logging in to your accounts, see [Logging into the CLI](#).

**Tip:** You can either run `cf ic` commands or `docker` commands to set up a Liberty server in a Docker container. For more information about `cf ic` commands and `docker` commands, see the Step 5 section of [Logging into the CLI](#).

### Procedure

1. To access your remote Liberty server in a Docker container, use the following command:

```
docker exec -i ContainerID LibertyInstallDirectory/bin configUtility install remoteAdministration --vadminUser=User
```

**Remember:** To find the container ID, use the `docker ps` command. By default, the `KeystorePassword` value is `Liberty`.

Also, by default the `LibertyInstallDirectory` value is `/opt/ibm/wlp`, and the `bin` directory is in the `/opt/ibm/wlp` directory.

For more information about the `configUtility` command, see [Liberty: configUtility command](#).

2. When the script displays the configuration snippet, copy it into the `remoteAdministration.xml` file. The `remoteAdministration.xml` file is in the `LibertyInstallDirectory/usr/servers/serverName/configDropins/defaults` directory. If this directory and file do not exist, create the directory and then create the file.
3. Specify the `<remoteFileAccess>` parameter in the `remoteAdministration.xml` file by replacing its contents with the following text:

```
<writeDir>${server.config.dir}</writeDir>
<writeDir>${server.output.dir}</writeDir>
<writeDir>${wlp.user.dir}</writeDir>
```

4. Save the `remoteAdministration.xml` file.

## What to do next

You can configure and start a remote Liberty server that is in a Docker container.

For more information about how to configure and start a remote Liberty server, see “Creating a remote Liberty server by using developer tools” on page 1427.

---

## Liberty and Chef

Chef software is an open source configuration management tool that you can use to create and manage the installation of an Infrastructure as a Service (IaaS). You can use Chef to provision a Liberty installation.

Chef uses cookbooks, which are reusable sets of components that are written in the Ruby programming language. A cookbook provides all the necessary components that are needed to configure an associated piece of software, for example, Apache HTTP Server. An important distinction between using Chef and writing scripts is the ability of Chef to determine the differences between the current software configuration and a new configuration and make only the changes necessary to move from one to the other. For more information, see the online Chef documentation [About Cookbooks](#).

By using Chef, you can create scalable infrastructure with minimal configuration to maintain. You can easily expand your existing infrastructure, for example, by creating and starting a new application server or web server. Chef automatically connects the new servers into the existing infrastructure as necessary.

The `wlp` cookbook installs and configures the WebSphere Application Server Liberty. It provides recipes, resources, and libraries for creating, managing, and configuring Liberty server instances. For more information, see `wlp` cookbook.

To learn more about Chef, see the online Chef documentation [How Chef works](#).

To learn more about using Chef cookbooks, see [Getting started with the Chef cookbooks for Liberty](#).

---

## Installing the OpenShift Cartridge for Liberty

Distributed operating systems

IBM i

8.5.5.9

The downloadable OpenShift cartridge allows the Liberty server to be available on OpenShift.

### Before you begin

- You must have Ruby version 1.9.3 or later installed.
- This document details how to download the OpenShift cartridge by using the Linux command line.

### About this task

OpenShift is an open source platform that allows developers to quickly develop, build, deploy, and manage Linux containerized services and applications in a cloud environment. When you install the OpenShift cartridge for Liberty, both Liberty and JRE binary files are downloaded for each application.

The OpenShift cartridge is also available at <https://github.com/WASdev/cloud.openshift.cartridge.wlp> where you can find extra documentation.

For more information about OpenShift and its advantages, see OpenShift

**Note:** Only OpenShift version 2 can be used with this cartridge

## Procedure

Installing the cartridge into your OpenShift environment

1. Download the cartridge compressed file from IBM Fix Central.
2. Run the **unzip** command to extract the contents of the cartridge `ibm-websphere-liberty-cartridge-v*.zip` file to the following cartridge directory `cloud.openshift.cartridge.wlp`
3. The OpenShift cartridge downloads the default Liberty and IBM JRE binary files for development only. If you have licenses for other binary files that you want to use, they need to be accessible with HTTP. See “Structure a Liberty repository for personal binary files” on page 1421 for details on how to structure this repository.
  - a. Update the `ibm-websphere-liberty-buildpack/config/ibmjdk.yml` file to point to your JRE binary.
  - b. Update the `ibm-websphere-liberty-buildpack/config/liberty.yml` file to point to your Liberty binary.
4. Run the **chmod u+x ibm-websphere-liberty-buildpack/resources/download\_buildpack\_cache.rb** command and add the binary files from step 3 to the cartridge cache. Run the **ibm-websphere-liberty-buildpack/resources/download\_buildpack\_cache.rb ibm-websphere-liberty-buildpack/admin\_cache**
5. If you are licensed to deploy the cartridge into your environment, you can create a `ibm-websphere-liberty-buildpack/config/licenses.yml` file that contains the accepted license numbers before packaging.

```
IBM_JVM_LICENSE: <jvm license code>
IBM_LIBERTY_LICENSE: <liberty license code>
```

**Note:** When installed the cartridge can be made available to all users. If you are an administrator or own your OpenShift installation, you can have more control over how the cartridge behaves in these situations. After you add the license to the cartridge package, individual applications do not need to accept the license terms with environment variables.

6. Return to your original directory and copy the cartridge directory to each node host on your OpenShift machines.
  7. On each node host run:

```
oo-admin-cartridge --action install --source cloud.openshift.cartridge.wlp/
service ruby193-mcollective restart
```
  8. On the broker host run:

```
oo-admin-broker-cache --clear --console
oo-admin-ctl-cartridge -c import-node --activate
oo-admin-console-cache --clear
```
  9. Verify that the cartridge is installed by running the **rhc cartridges** command.
- Uninstalling the cartridge from your OpenShift environment
10. On the broker host run:

```
oo-admin-ctl-cartridge -c deactivate --name ibm-liberty-8.5.5
```
  11. On each node host run:

```
oo-admin-cartridge --action erase --name liberty --version 8.5.5 --cartridge_version <Cart_Version_Number>
```
  12. On the broker host run:

```
oo-admin-broker-cache --clear --console
oo-admin-console-cache --clear
```
  13. Verify that the cartridge uninstalled by running the **rhc cartridges** command.

## Results

The OpenShift cartridge is now installed.

---

# Installing the IBM WebSphere Application Server Liberty Buildpack into a Cloud Foundry Environment

Distributed operating systems

IBM i

8.5.5.9

The IBM WebSphere Application Server Liberty Buildpack makes the Liberty server available in Cloud Foundry.

## Before you begin

- You must have Ruby version 1.9.3 or later installed.
- This document details how to download the IBM WebSphere Application Server Liberty buildpack by using the Linux command line.

## About this task

Use this task to install the IBM WebSphere Application Server Liberty Buildpack into a Cloud Foundry Environment. If you are a Cloud Foundry administrator, you can install the Liberty buildpack as an admin buildpack making it available to all users within the Cloud Foundry.

**Note:** Buildpack users do not need to specify the `-b` option to use the buildpack directly from the administrator.

The IBM WebSphere Application Server Liberty Buildpack is also available at <https://github.com/cloudfoundry/ibm-websphere-liberty-buildpack> where you can find extra documentation.

## Procedure

Installing the buildpack into your Cloud Foundry environment

1. Download the buildpack compressed file from IBM Fix Central.
2. Run the **unzip** command to extract the contents of the buildpack `ibm-websphere-liberty-buildpack-v*.zip` file to the following buildpack directory `ibm-websphere-liberty-buildpack`
3. The IBM WebSphere Application Server Liberty buildpack downloads the default Liberty and IBM JRE binary files for development only. If you have licenses for other binary files that you want to use, they need to be accessible with HTTP. See “Structure a Liberty repository for personal binary files” on page 1421 for details on how to structure this repository.
  - a. Update the `config/ibmjdk.yml` file to point to your JRE binary.
  - b. Update the `config/liberty.yml` file to point to your Liberty binary.
4. If you are licensed to deploy the buildpack into your environment, you can create a `config/licenses.yml` file that contains the accepted license numbers before packaging.

```
IBM_JVM_LICENSE: <jvm license code>
IBM_LIBERTY_LICENSE: <liberty license code>
```

**Note:** After you add the license to the buildpack package, individual applications do not need to accept the license terms with environment variables.

5. Install Ruby gems that are needed to package an admin buildpack by running the **gem install bundler** and **bundle install** commands.
6. Run the **bundle exec rake** package task to create an admin buildpack.

```
rake 'package[zipfile,hosts,version]'
```

The **zipfile** parameter is the name of the generated admin buildpack and includes a relative location that is NOT the current directory. For example, `../my-admin-buildpack.zip` can be specified as the **zipfile** parameter to generate the `my-admin-buildpack.zip` file in the parent directory instead of the default `ibm-websphere-liberty-buildpack-480d2de.zip` file.

For example,

```
rake 'package[../my-admin-buildpack.zip]'
```

The **hosts** parameter is a list of sites that the package task pulls binary files from for inclusion in the admin buildpack. By default, only binary files from the public IBM site are pulled. IBM hosted sites do not include third-party binary files. A package parameter must be specified to indicate that third-party binary files can be included in the admin buildpack for cases where the admin buildpack is used in offline mode. Using `*` includes all the binary files in the admin buildpack if the download is possible during the packaging.

An example of this usage:

```
rake 'package[,*,]'
```

The **version** parameter is the version information that is displayed when an application is deployed to **CloudFoundry** with the Cloud Foundry command line interface. By default, the displayed version is the latest commit identifier, such as `480d2de`.

The following example illustrates the displayed version information defaults.

```
Liberty Buildpack Version: 480d2de | git@github.com:cloudfoundry/ibm-websphere-liberty-buildpack.git#480d2de
```

7. Install the admin buildpack with the `cf` client as follows:

```
cf create-buildpack ibm-websphere-liberty-buildpack ibm-websphere-liberty-buildpack-480d2de.zip 1
```

- `ibm-websphere-liberty-buildpack` is the name that is given to the admin buildpack.
- `ibm-websphere-liberty-buildpack-480d2de.zip` is the path to the compressed file that is created by the Rake task.
- `1` is the priority given to the admin buildpack. The lower the number, the higher the priority.

See the Cloud Foundry documentation for further details.

## Results

The IBM WebSphere Application Server Liberty Buildpack is now installed.

## Structure a Liberty repository for personal binary files

8.5.5.9

The OpenShift cartridge and the IBM WebSphere Application Server Liberty Buildpack both download the default Liberty and IBM JRE binary files for development only. If you want to use your own binary files that you have other licenses for, the files must be accessible with HTTP.

### Repository structure

The repository is an HTTP-accessible collection of files. The repository root must contain an `index.yml` file that is a mapping of concrete versions to absolute URIs. For example,

```
<version>:
  uri: <URI of binary>
  license: <URI of license>
```

You can store your files in the repository. For example,

```
/index.yml
/ibm-java-jre-7.0-5.0-x86_64-archive.bin
/ibm-java-jre-7.0-5.0-x86_64-License.html
```

Versions are composed of the following four parts: major, minor, micro, and optional qualifier. The version format is <major>.<minor>.<micro>[\_<qualifier>].

Table 103. Part Requirements

Part	Requirement
Major	Numeric
Minor	Numeric
Micro	Numeric
Optional qualifier	Letters, digits, and hyphens with lexical order: <ol style="list-style-type: none"> <li>1. Hyphen</li> <li>2. Lowercase letter</li> <li>3. Uppercase letters</li> <li>4. Digits</li> </ol>

Aside from declaring a specific version to use, you can also specify a bounded range of versions. You can append the + symbol to a version prefix to use the latest version that begins with the prefix.

Table 104. Version Declarations

Example	Description
1.+	Selects the greatest available version less than 2.0.0.
1.7.+	Selects the greatest available version less than 1.8.0.
1.7.0+	Selects the greatest available version less than 1.7.1. <b>Note:</b> Use this syntax to stay up to security releases in a particular version.

For examples of `index.yml` files that illustrate the guidelines for the repository structure detailed in this document, see

<https://public.dhe.ibm.com/ibmdl/export/pub/software/websphere/wasdev/downloads/wlp/index.yml>

<https://public.dhe.ibm.com/ibmdl/export/pub/software/websphere/wasdev/downloads/jre/index.yml>

---

## Chapter 5. Setting up Liberty

Define directory locations and variables, create and configure servers, and add and remove Liberty features that specify the capabilities of your server.

### Procedure

- Defining directory locations and properties.
- **8.5.0.1** “Verifying the integrity of Liberty installation” on page 1414.
- **Distributed operating systems** “Creating a Liberty server by using developer tools” on page 1424.
- “Creating a Liberty server manually.”
- “Specifying Liberty bootstrap properties” on page 1437.

The default HTTP port is 9080 and HTTPS port is 9443 for Liberty. You can manually assign appropriate port numbers in the `server.xml` files when multiple Liberty servers are running on the same machine.

---

## Creating a Liberty server manually

You can create a server from the command line.

### **Distributed operating systems**

#### Before you begin

### **Distributed operating systems**

You can create a server as described here, or as described in “Creating a Liberty server by using developer tools” on page 1424.

### Procedure

1. Open a command line, then change directory to the `wlp/bin` directory.  
Where *path\_to\_liberty* is the location you installed Liberty on your operating system.  
Example on Windows: `C:\Users\mo> cd path_to_liberty\wlp\bin`  
Example on Linux: `mo@machine01:~> cd path_to_liberty/wlp/bin`
2. Run the following command to create a server. If you do not specify a server name, `defaultServer` is used.

Where *server\_name* is the name you want to give your server.

Example on Windows: `C:\wlp\bin> server create server_name`

Example on Linux: `mo@machine01:~> server create server_name`

Windows

AIX

Linux

UNIX

HP-UX

Solaris

z/OS

IBM i

```
server create server_name
```

*server\_name* must use only Unicode alphanumeric (for example, 0-9, a-z, A-Z), underscore (`_`), dash (`-`), plus (`+`), and period (`.`) characters. The name cannot begin with a dash or period. Your file system, operating system, or compressed file directory might impose additional restrictions.

## Results

If the server is created successfully, you receive message: Server *server\_name* created.

If the specified server already exists, no server is created and you receive an exception message:

```
CWWKE0005E: The runtime environment could not be launched.  
CWWKE0045E: It was not possible to create the server called server_name because  
the server directory C:\wlp\usr\servers\server_name already exists.
```

A directory with the name of the new server is created under the `${wlp.user.dir}/servers` directory, containing the configuration of the new server. The HTTP port numbers for the new server are assigned to default values and are shown in the generated `server.xml` file to make it easy to edit them. You can also set these values by using variables in a `bootstrap.properties` file in the same directory. For more information, see “Specifying Liberty bootstrap properties” on page 1437.

## What to do next

Configure your server to have the features that your application requires. See “Configuring the Liberty runtime environment ” in the “Administering” book.

---

## Creating a Liberty server by using developer tools

### Distributed operating systems

You can use developer tools to create and start a Liberty server. If you have not yet installed Liberty, the developer tools can install it for you when you create a server for the first time.

## Before you begin

Make sure that you installed the developer tools as described in “Installing Liberty developer tools and (optionally) Liberty” on page 1374.

You can create a server as described in this topic, or as described in “Creating a Liberty server manually” on page 1423.

When you create a new server using the tools, you specify the installation of Liberty that you want to use. You are offered three options:

- **Select an existing installation.**
- **Install from a previously downloaded archive file.**
- For the no-charge developer edition, **Download and install.**

If you want to use the tools to install a Liberty edition (other than the no-charge developer edition) from an archive file, make sure that you have downloaded the archive file.



8.5.5.5

If you need to use a proxy server to connect to the Liberty repository, first configure the proxy settings by selecting **Window > Preferences > General > Network Connections** from the main menu in Eclipse. Enter the information there.

## About this task

Complete the following steps to create and start a Liberty server.

As you go through the steps, you can download add-ons in the Liberty Repository from the WASdev community download site.

## Procedure

1. In the workbench, open the Servers view by clicking the **Servers** tab.

**Tip:** If the Servers view is not visible, navigate to **Window > Show view > Other...** and type **Server** in the filter text. Then, select **Servers**.

2. Right-click the **Servers** view and select **New > Server**.
3. Under the server type list, expand **IBM** and select the  **8.5.5.4 WebSphere Application Server Liberty** server type.  **8.5.5.4** The WebSphere Application Server Liberty server type replaces the old WebSphere Application V8.5 Liberty server type and supports all versions of the WebSphere Application Server Liberty server. Existing servers in a workspace that were created with the old server type still work.
4. Click **Next**. The Liberty Runtime Environment page is displayed.
- 5.

**Tip:** If you already have a Liberty run time that is installed, you will go directly to the **New Remote Liberty Server** page, skip to Step 7.

Select an installation, install from an archive file, or (for the no-charge developer edition) download and install, Liberty.

If you previously installed Liberty, complete the following steps:

- a.  **8.5.5.4** Select **Choose an existing installation**.
- b.  **8.5.5.4** In the **Path** field, type or browse for the directory where you installed the Liberty runtime environment.
- c.  **8.5.5.4** On the Liberty Runtime Environment page, click **Next**.  
The application-serving environment is selected, and now you can skip to Step 7.

If you want to install Liberty from an archive file that was previously downloaded, complete the following steps:

- a.  **8.5.5.4** Select **Install from an archive or repository**, and click **Next**.
- b.  **8.5.5.4** In the **Destination** field, type or browse for the directory where you want to install the Liberty runtime environment.  
If you type a path that does not exist, then a folder for that path is created automatically at the end of Step 10.
- c.  **8.5.5.4** Select **Install a new runtime environment from an archive**.
- d.  **8.5.5.4** In the **Path** field, either type or browse to the archive file on the local file system, and click **Next**.
- e. In the Install Add-ons page, click **Install** or **Install Pending** to make your selection of add-on archive files that you want to install on the Liberty runtime environment.

You can install an add-on archive file from your local file system, download, or use a combination of both when you install multiple add-on archive files. If the workbench is connected to the internet, the Install Add-ons page is populated with add-on archive files available for download from the WAS dev community download site.

This download site includes add-ons that you can select from the Liberty Repository, such as runtime features, samples, or open source integration.

If you want to install add-on archive files from your local file system, click **Add Archive**. In the **Add-on archive** field, type or browse for the add-on archive file on the local file system, and then click **OK**. If you have more add-on archive files to install from your local file system, repeat this step until you are done.



8.5.5.6

If you want to install add-on files from a custom repository, first add the repository by clicking **Configure Repositories**. Click **New...** to add the repository. The files are then added to the list of add-on files.

After you complete your selection in the Install Add-ons page, click **Next**.

- f. In the License Acceptance page, if you accept the license terms, select **I accept the terms of all the license agreements** then click **Next**.

Now you can skip to Step 7.

If you want to download and install the no-charge developer edition of Liberty, complete the following steps:



8.5.5.4

- a. Select **Install from an archive or repository**, and click **Next**.



8.5.5.4

- b. In the **Destination** field, type or browse for the directory where you want to install the Liberty runtime environment.

If you type a path that does not exist, then a folder for that path is created automatically at the end of Step 10.



8.5.5.4

- c. Select **Download and install a new runtime environment from ibm.com**, choose a runtime environment version, and then click **Next**.

- d. In the Install Add-ons page, click **Install** or **Install Pending** to make your selection of add-on archive files that you want to install on the Liberty runtime environment.

You can install an add-on archive file from your local file system, download, or use a combination of both when you install multiple add-on archive files. If the workbench is connected to the internet, the Install Add-ons page is populated with add-on archive files available for download from the WAS dev community download site.

This download site includes add-ons that you can select from the Liberty Repository, such as runtime features, samples, or open source integration.

If you want to install add-on archive files from your local file system, click **Add Archive**. In the **Add-on archive** field, type or browse for the add-on archive file on the local file system, and then click **OK**. If you have more add-on archive files to install from your local file system, repeat this step until you are done.

If you want to install add-on files from a custom repository, first add the repository by clicking **Configure Repositories**. Click **New...** to add the repository. The files are then added to the list of add-on files.

After you complete your selection in the Install Add-ons page, click **Next**.

- e. In the License Acceptance page, if you accept the license terms, select **I accept the terms of all the license agreements** then click **Next**.

Now you can skip to Step 7.

- 6. If the Liberty Server page displays, in the **Liberty server** field, use the drop-down list to select an existing server. Or click **New** to create a new server.

**Note:** This step is skipped and the New Liberty Server dialog is displayed directly if there are no defined Liberty Servers to choose from.

- 7. If you are creating a new server, in the **Server name** field of the New Liberty Server page, enter a server name of your choice or use the default server name, defaultServer. Then, click **Next** if available, otherwise click **Finish**.
- 8. In the Liberty Server, click **Next**.
- 9. Optional: Add the projects of your application to the server. On the **Add and Remove** page, under the **Available** list, select the projects that you want to add to the server and click **Add**. The project appears in the **Configured** list.
- 10. Click **Finish**.

## What to do next

- Edit the server configuration. For more information, see topic “Editing the Liberty configuration by using developer tools” in the “Administering” book.
- Start the server in “start” mode or in “debug” mode, stop the server, add or remove applications on the server, and many other tasks. You can perform these tasks by using the server context menu (right-click on the server to open the pop-up menu) or by selecting the tray buttons in the Servers view.

**Tip:** In the Servers view, you must select the server entry to perform these tasks. Do not select the server configuration, such as the Server Configuration [server.xml] entry for performing these tasks.

- Optionally configure your server to do specific tasks such as configure Liberty to authenticate users with Tivoli Directory Server: Right-click **Servers**. Select **Utilities> Add config snippets**. After you select the snippets and accept any licenses, the selected configuration snippets are then downloaded and included in the **server.xml** file.

---

## Creating a remote Liberty server by using developer tools

Distributed operating systems



8.5.5.4

You can use developer tools to create and start a remote Liberty server.

### Before you begin

You must meet prerequisites for your local system and your remote system.

- The local system refers to the system where you installed the developer tools.
- The remote system refers to the system where you have Liberty runtime environment that is installed and a Liberty server created.

For your local system, ensure that you meet these prerequisites:

1. The developer tools are installed.

For more information, see “Installing Liberty developer tools and (optionally) Liberty” on page 1374.

2. The Liberty runtime environment is installed. For more information, see “Installing and uninstalling Liberty using downloaded files and archives” on page 1371.

For your remote system, ensure that you call the `configUtility` to download and set up the `remoteAdministration` snippet from the repository. Copy the config text that is retrieved by the `configUtility` into the `server.xml` file. For more information, see “Liberty:configUtility command” on page 1575.

You can use the following sample remote configuration as an example for your `server.xml` file:

```
<server description="new server">
<!-- Enable features-->
<featureManager>
<feature>restConnector-1.0</feature>
</featureManager>

<keyStore id="defaultKeyStore" password="password" />

<quickStartSecurity userName="admin" userPassword="password"/>

<httpEndpoint id="defaultHttpEndpoint" host="*" httpPort="9080" httpsPort="9443"/>

<remoteFileAccess>
<writeDir>${server.config.dir}</writeDir>
```

```
<writeDir>${server.output.dir}</writeDir>
<writeDir>${wlp.user.dir}</writeDir>
</remoteFileAccess>
</server>
```

## Procedure

1. In the workbench, open the Servers view by clicking the **Servers** tab.

**Tip:** If the Servers view is not visible, navigate to **Window > Show view > Other...** and type **Server** in the filter text. Then, select **Servers**.

2. Right-click within the **Servers** view and select **New > Server**.
3. Under the server type list, expand **IBM** and select the **WebSphere Application Server Liberty** server type.
4. Enter the host name of the remote server.
5. Click **Next**. The Liberty Runtime Environment page is displayed.
- 6.

**Tip:** If you already have a Liberty run time that is installed, you will go directly to the **New Remote Liberty Server** page, skip to Step 7.

Select an installation, install from an archive file, or (for the no-charge developer edition) download and install Liberty.

If you previously installed Liberty, complete the following steps:

- a.  **8.5.5.4** Select **Choose an existing installation**.
- b.  **8.5.5.4** In the **Path** field, type or browse for the directory where you installed the Liberty runtime environment.
- c.  **8.5.5.4** On the Liberty Runtime Environment page, click **Next**.

The application-serving environment is selected, and now you can skip to Step 7.

If you want to install Liberty from an archive file that was previously downloaded, complete the following steps:

- a.  **8.5.5.4** Select **Install from an archive or repository**, and click **Next**.
- b.  **8.5.5.4** In the **Destination** field, type or browse for the directory where you want to install the Liberty runtime environment.  
If you type a path that does not exist, then a folder for that path is created automatically at the end of Step 12.
- c.  **8.5.5.4** Select **Install a new runtime environment from an archive**.
- d.  **8.5.5.4** In the **Path** field, either type or browse to the archive file on the local file system, and click **Next**.
- e. In the Install Add-ons page, click **Install** or **Install Pending** to make your selection of add-on archive files that you want to install on the Liberty runtime environment.

You can install an add-on archive file from your local file system, download, or use a combination of both when you install multiple add-on archive files. If the workbench is connected to the internet, the Install Add-ons page is populated with add-on archive files available for download from the WAS dev community download site.

This download site includes add-ons that you can select from the Liberty Repository, such as runtime features, samples, or open source integration.

If you want to install add-on archive files from your local file system, click **Add Archive**. In the **Add-on archive** field, type or browse for the add-on archive file on the local file system, and then click **OK**. If you have more add-on archive files to install from your local file system, repeat this step until you are done.

If you want to install add-on files from a custom repository, first add the repository by clicking **Configure Repositories**. Click **New...** to add the repository. The files are then added to the list of add-on files.

After you complete your selection in the Install Add-ons page, click **Next**.

- f. In the License Acceptance page, if you accept the license terms, select **I accept the terms of all the license agreements** then click **Next**.

Now you can skip to Step 7.

If you want to download and install the no-charge developer edition of Liberty, complete the following steps:

- a.  **8.5.5.4** Select **Install from an archive or repository**, and click **Next**.
- b.  **8.5.5.4** In the **Destination** field, type or browse for the directory where you want to install the Liberty runtime environment.  
If you type a path that does not exist, then a folder for that path is created automatically at the end of Step 12.
- c.  **8.5.5.4** Select **Download and install a new runtime environment from ibm.com**, choose a runtime environment version, and then click **Next**.
- d. In the Install Add-ons page, click **Install** or **Install Pending** to make your selection of add-on archive files that you want to install on the Liberty runtime environment.

You can install an add-on archive file from your local file system, download, or use a combination of both when you install multiple add-on archive files. If the workbench is connected to the internet, the Install Add-ons page is populated with add-on archive files available for download from the WAS dev community download site.

This download site includes add-ons that you can select from the Liberty Repository, such as runtime features, samples, or open source integration.

If you want to install add-on archive files from your local file system, click **Add Archive**. In the **Add-on archive** field, type or browse for the add-on archive file on the local file system, and then click **OK**. If you have more add-on archive files to install from your local file system, repeat this step until you are done.

If you want to install add-on files from a custom repository, first add the repository by clicking **Configure Repositories**. Click **New...** to add the repository. The files are then added to the list of add-on files.

After you complete your selection in the Install Add-ons page, click **Next**.

- e. In the License Acceptance page, if you accept the license terms, select **I accept the terms of all the license agreements** then click **Next**.

Now you can skip to Step 7.

7. Complete the user ID, password, and port information for the remote server and click **Verify**.

**Important:**

- The user ID and password must have the appropriate security credentials as defined by the quickStartSecurity configuration item or the user registry of the remote Liberty server.
- The port is the HTTPS port that is configured in the server.xml file.

After you click **Verify**, if you see the following message, a local server or remote server is already created with the same name.

You can verify this situation by expanding the following folders in the Enterprise Explorer view and seeing the listed servers in the following projects:

- WebSphere Application Server Liberty
- WebSphere Application Server Liberty (Remote)

The remote directory is shown on the same page if the connection is successful. To resolve this issue of two servers with the same name, you can rename the Remote Directory folder on the remote system.

8. In the New Remote Liberty Server page, click **Next**.

The Remote WebSphere Application Server Settings page is displayed.

9. If you do not want to enable remote start, stop, and restart, ensure that **Enable the server to start remotely** is cleared, click **Next**, and skip the next step.

10. Enable remote start, stop, and restart.

- a. Select **Enable the server to start remotely**.
- b. Select whether your remote server is installed on the Windows operating system or other operating systems.
- c. Enter the location of the runtime installation and server configuration.

For more information, see the “Liberty:Directory locations and properties” on page 1434 topic.

- d. Enter the remote server authentication information.

For authentication, complete one of the following options.

- To access the remote server with logon credentials, enter your user name and password.
- To access the remote server with Secure Sockets Layer (SSL), copy the private key file to the computer where the workbench is installed, and specify the key file location and user ID.

For more information about starting a remote server, see the Starting a remote WebSphere Application Server topic.

11. Optional: Add the projects of your application to the server. On the **Add and Remove** page, under the **Available** list, select the projects that you want to add to the server and click **Add**. The project appears in the **Configured** list.
12. Click **Finish**.

## What to do next

- Edit the server configuration. When you make edits, the remote servers synchronize configuration changes with the remote version of the file. If the configuration files are out of sync with the remote server, then the developer tools prompt you before they overwrite any remote files. For more information, see topic “Editing the Liberty configuration by using developer tools” in the “Administering” book.
- Start the server in “start” mode or in “debug” mode, stop the server, add or remove applications on the server, and many other tasks. You can perform these tasks by using the server menu (right-click on the server to open the pop-up menu) or by selecting the tray buttons in the Servers view.

**Tip:** In the Servers view, you must select the server entry to perform these tasks. Do not select the server configuration, such as the Server Configuration [server.xml] entry for performing these tasks.

---

## Creating a workbench Liberty server in a Docker container by using developer tools

You can use WebSphere Developer Tools to create a reference in the workbench to a Liberty server that is running in a Docker container. You can use this reference to handle your server requests from the workbench.

## Before you begin

- Install WebSphere Developer Tools. For more information about installing WebSphere Developer Tools, see *Installing the Liberty developer tools and (optionally) Liberty*.
- Start a Liberty server in a local Docker container and ensure that both the HTTP and HTTPS ports are mapped to the host. For more information about starting a Liberty server in a local Docker container, see *WASdev GitHub*.

## About this task

**Remember:** You can create a reference in the workbench to a Liberty server that is running in a Docker container.

As you complete the steps, you can install WebSphere Application Server Liberty and download add-ons in the Liberty Repository from the WASdev community download site. After you install Liberty, you can select your Docker container. Then, you can enter the Liberty server security credentials for your Liberty server to create a workbench reference to your Liberty server in your Docker container.

## Procedure

1. In the workbench, open the Servers view by clicking the **Servers** tab.

**Tip:** If the Servers view is not visible, select **Window > Show view > Other...** and type **Server** in the filter text. Then, select **Servers**.

2. Right-click the **Servers** view and select **New > Server**.
3. To select your server type, select **IBM > WebSphere Application Server Liberty**.
4. Enter the localhost value in the **Server's host name** field.
5. Click **Next**.
6. If the tools prompt you to install WebSphere Application Server Liberty, either because it is not installed or because you need to input the directory where it is installed, complete one of the following options. Otherwise, skip this step.

You need Liberty to be installed so that you can create a workbench reference to a Liberty server in a Docker container.

If you previously installed Liberty, complete the following steps to select the directory where you installed it:

- a. Select **Choose an existing installation**.
- b. In the **Path** field, type or browse for the directory where you installed the WebSphere Application Server Liberty.
- c. On the Liberty Runtime Environment page, click **Next**.

The application-serving environment is selected. Skip the rest of this step.

If you want to install Liberty from an archive file that was previously downloaded, complete the following steps:

- a. Select **Install from an archive or repository**, and click **Next**.
- b. In the **Destination** field, type or browse to the directory where you want to install the Liberty runtime environment.

If you type a path that does not exist, then a folder for that path is created automatically at the end of the procedure when you click **Finish**.

- c. Select **Install a new runtime environment from an archive**.
- d. In the **Path** field, either type or browse to the archive file on the local file system, and click **Next**.

- e. In the Install Add-ons page, click **Install** or **Install Pending** to make your selection of add-on archive files that you want to install on the Liberty runtime environment.

You can install an add-on archive file from your local file system, download an add-on archive file, or use a combination of both when you install multiple add-on archive files. If the workbench is connected to the internet, the Install Add-ons page is populated with add-on archive files available for download from the WAS dev community download site.

This download site includes add-ons that you can select from the Liberty Repository, such as runtime features, samples, or open source integration.

If you want to install add-on archive files from your local file system, complete the following steps:

- 1) Click **Add Archive**.
- 2) In the **Add-on archive** field, type or browse to the add-on archive file on the local file system.
- 3) Click **OK**.

If you have more add-on archive files to install from your local file system, repeat this procedure until you are done.

If you want to install add-on files from a custom repository, complete the following steps:

- 1) To add the repository, click **Configure Repositories**.
- 2) Click **New...**

The files are then added to the list of add-on files.

After you complete your selection in the Install Add-ons page, click **Next**.

- f. In the License Acceptance page, if you accept the license terms, select **I accept the terms of all the license agreements** then click **Next**.

If you want to download and install the no-charge developer edition for Liberty, complete the following steps:

- a. Select **Install from an archive or repository**, and click **Next**.
- b. In the **Destination** field, type or browse to the directory where you want to install the Liberty runtime environment.

If you type a path that does not exist, then a folder for that path is created automatically at the end of the main procedure when you click **Finish**.

- c. Select **Download and install a new runtime environment from ibm.com**, choose a runtime environment version, and then click **Next**.
- d. In the Install Add-ons page, click **Install** or **Install Pending** to make your selection of add-on archive files that you want to install on the Liberty runtime environment.

You can install an add-on archive file from your local file system, download, or use a combination of both when you install multiple add-on archive files. If the workbench is connected to the internet, the Install Add-ons page is populated with add-on archive files available for download from the WAS dev community download site.

This download site includes add-ons that you can select from the Liberty Repository, such as runtime features, samples, or open source integration.

If you want to install add-on archive files from your local file system, click **Add Archive**. In the **Add-on archive** field, type or browse for the add-on archive file on the local file system, and then click **OK**. If you have more add-on archive files to install from your local file system, repeat this step until you are done.

If you want to install add-on files from a custom repository, first add the repository by clicking **Configure Repositories**. Click **New...** to add the repository. The files are then added to the list of add-on files.

After you complete your selection in the Install Add-ons page, click **Next**.

- e. In the License Acceptance page, if you accept the license terms, select **I accept the terms of all the license agreements** then click **Next**.

7. On the Liberty Server Type page, select **Server in a Docker container**.
8. Click **Next**.  
The tools display the New Liberty Server in Docker Container page.
9. Select your Docker container from the **Container name** menu.
10. Enter the Liberty server security credentials.  
Your values for the **User name** and **Password** fields must correspond to a user that is defined in a user registry that has an administrator role. If the tools cannot find a basic user registry that defines the specified user, the tools display the Security Verification window. If the tools display the Security Verification window, complete one of the following options:
  - Select **Create** to add a basic user registry that defines a user with your values and an administrator role.
  - Select **Proceed** to proceed if the user is defined in another user registry type.
  - Select **Cancel** to make changes to the **User name** and **Password** that you entered.
11. Enter the value for the **Host mapped secured port** field that corresponds to the HTTPS port in the server configuration.
12. Click **Finish**.

## Results

You created a workbench server reference to a server that is running in a Docker container.

- To see the server that you created and its server configuration, open the Servers view.
- To see the project, the server folder, and the server configuration files, open the Enterprise Explorer view.

## What to do next

- You can edit the server configuration. For more information, see “Editing the Liberty configuration by using developer tools” on page 1556
- To start or stop a server, or add or remove applications on the server, right-click your server to use the server context menu or use the tray buttons in the Servers view. For more information, see “Starting and stopping a server by using developer tools” on page 1558.

**Remember:** To access these options, select the **Server Entry** in the Servers view. Do not select a server configuration such as the **Server Configuration** or `server.xml` entry.

**Tip:** The application address that the server logs in the Console view is valid within the Docker container only. To load an application in a browser, use the host mapped IP address and host mapped HTTP or HTTPS port. If you use the **Run on Server** or **Debug on Server** options, the application is automatically loaded with the correct IP address and port.

To make it easier to determine the correct port, map the ports to specific ports on the host by using the `-p` option rather than the `-P` option when you create the Docker container.

- You can configure your Liberty server to authenticate users with Tivoli Directory Server.
  1. Right-click **Servers**.
  2. Select **Utilities > Add config snippets**.
  3. Select the snippets and accept the licenses agreements.

The tools download the configuration snippets that you selected and add them to the `server.xml` file.

## Liberty:Directory locations and properties

In Liberty, many directories have properties that are associated with them. These properties can be used to specify file locations when you configure the server.

*Table 105. Runtime environment default directory structure.* Column 1 contains a file and directory tree. If a directory has a property that is associated with it, this is given in column 2. A description of each file or directory is given in Column 3.

Directory or file	Property	Description
wlp/ +- bin/ +- clients/ +- jython/ +- dev/ +- api/ +- ibm/ +- javadoc/ +- spec/ +- third-party/  +- spi/ +- ibm/ +- javadoc/ +- spec/ +- tools/ +- etc/ +- server.env +- client.env +- jvm.options +- lafiles/ +- lib/ +- templates/  8.5.5.6 +- client/	wlp.install.dir	Root of installation  Scripts for managing the installation. For example, server.  Liberty client and thin client libraries. For example restConnector.jar.  Jython-based scripts  Root for developer resources (APIs, SPIs, specifications, and tools)  Public APIs available for both compile and run time by default  APIs available in Liberty  Java document archives  Public specification APIs available for both compile and run time by default  Third-party APIs that are available at compile time by default and must be specified in the configuration using the apiTypeVisibility attribute of the classloader element for applications at run time.  Public SPIs available for both compile and run time by default  SPIs available in Liberty  Java document archives for SPI  Public specification SPIs available for both compile and run time by default  Ant plug-in for Liberty  User customized server variables that apply to all servers (optional)  Default server script environment variables (optional)  Default client script environment variables (optional)  Default JVM options (optional)  License information files  Platform runtime environment  Runtime customization templates and examples  8.5.5.6 Client template when creating a client

Table 105. Runtime environment default directory structure (continued). Column 1 contains a file and directory tree. If a directory has a property that is associated with it, this is given in column 2. A description of each file or directory is given in Column 3.

Directory or file	Property	Description
+ server/		Server template when creating a server
+ usr/	wlp.user.dir	User directory
+ extension/	usr.extension.dir	User-developed features
+ shared/		
+ apps/	shared.app.dir	Shared applications
+ config/	shared.config.dir	Shared configuration files
+ resources/	shared.resource.dir	Shared resource definitions: adapters, data sources
8.5.5.7 +- stackGroups/	shared.stackgroup.dir	Shared stack groups for remote deployment of packages and installables
+ servers/		Shared servers directory
+ server_name	server.config.dir	Server configuration directory. Use <code>\${server.config.dir}</code> to reference server-specific configuration (applications).
+ bootstrap.properties		Server bootstrap properties (optional)
+ jvm.options		Server JVM options, which replace the values in <code>wlp/etc/jvm.options</code> (optional)
+ server.env		Server script environment variables, which are merged with <code>wlp/etc/server.env</code> (optional)
+ server.xml		Server configuration overlays (required)
+ apps/		Server configuration for applications
+ dropins/		Server default application dropins folder (optional)
+ application_name		Application folder or archive (optional)
8.5.5.5 +- configDropins/		Server configuration dropins folder (optional)
8.5.5.5 +- defaults		Default server configuration dropins folder (optional)
8.5.5.5 +- overrides		Server configuration overrides dropins folder (optional)
+ server_name	server.output.dir	Server output directory. Use <code>\${server.output.dir}</code> to describe artifacts generated by the server (log files and workarea).
+ logs/		Server log files, including FFDC logs (directory is present after server is first run)
+ console.log		Basic server status and operations messages
+ trace_timestamp.log		Time-stamped trace messages, with the level of detail determined by the current tracing configuration

Table 105. Runtime environment default directory structure (continued). Column 1 contains a file and directory tree. If a directory has a property that is associated with it, this is given in column 2. A description of each file or directory is given in Column 3.

Directory or file	Property	Description
<pre> +- ffdc/     +- ffdc_timestamp/ +- workarea/                     </pre>		<p>First Failure Data Capture (FFDC) output directory</p> <p>First Failure Data Capture (FFDC) output that typically includes selective memory dumps of diagnostic data related to the failure of a requested operation</p> <p>Files created by the server as it operates (directory is present after server is first run)</p>
<pre> 8.5.5.6 +- clients/ +- client_name +- bootstrap.properties +- client.jvm.options  +- client.xml +- apps/ +- logs/  +- trace_timestamp.log  +- ffdc/     +- ffdc_timestamp/  +- workarea/                     </pre>		<p>Shared clients directory</p> <p>Client configuration directory.</p> <p>Client bootstrap properties (optional)</p> <p>Client JVM options, which replace the values in <code>wlp/etc/client.jvm.options</code> (optional)</p> <p>Client configuration overlays (required)</p> <p>Client configuration for applications</p> <p>Client log files, including FFDC logs (directory is present after client is first run)</p> <p>Time-stamped trace messages, with the level of detail determined by the current tracing configuration</p> <p>First Failure Data Capture (FFDC) output directory</p> <p>First Failure Data Capture (FFDC) output that typically includes selective memory dumps of diagnostic data related to the failure of a requested operation</p> <p>Files created by the client as it operates (directory is present after client is first run)</p>

You can use the properties that are associated with each directory, if any, to specify file locations when you configure the server.

**Tip:** To ensure configuration portability, use the most specific property that is appropriate, and do not rely on the relationship between resources. For example, in some configurations the installation location, `${wlp.install.dir}` might not be the parent of the customized instance `${wlp.user.dir}`.

## Programmatic access to location properties

Location properties can be bound into the JNDI namespace under names of your choice, using the `jndiEntry` configuration elements in the `server.xml` file, for example:

```
<jndiEntry jndiName="serverName" value="${wlp.server.name}"/>
```

Such entries are accessible by any code that runs in the server (applications, shared libraries or features) through a JNDI lookup:

```
Object serverName = new InitialContext().lookup("serverName");
```

For more information on how to use JNDI entries in configuration, see “Using JNDI binding for constants from the server configuration files” on page 2146.

Feature code can also use a system programming interface (SPI) provided by the kernel to resolve the values of these properties, for example:

```
ServiceReference <WsLocationAdmin>locationAdminRef = bundleContext.getServiceReference(WsLocationAdmin.class);  
WsLocationAdmin locationAdmin = bundleContext.getService(locationAdminRef);  
String serverName = locationAdmin.resolveString("${wlp.server.name}");
```

---

## Specifying Liberty bootstrap properties

Bootstrap properties initialize the runtime environment for a particular server. Generally, they are attributes that affect the configuration and initialization of the runtime core.

### About this task

Bootstrap properties are set in a text file named `bootstrap.properties`. This file is not required, so it does not exist unless you create it. You must create this file in the server directory, which also contains the configuration root file `server.xml`. By default, the server directory is `usr/servers/server_name`. You can change the server directory as described in [8.5.0.1](#) “Customizing the Liberty environment” on page 1565.

You can create a `bootstrap.properties` file by using the editor in WebSphere Application Server Developer Tools for Eclipse. From the **Servers** view, right-click on the server you want to configure, then select **New**, then **Server Environment File**, then `bootstrap.properties`, and the file is created from a template and opened in an editor. Along with the `server.xml` and `server.env` files, the `bootstrap.properties` file appears in the **Servers** view under the server that it is associated with and can be edited by double-clicking it.

You can edit the `bootstrap.properties` file by using a text editor or the editor in the WebSphere Application Server Developer Tools for Eclipse. See “Editing the Liberty configuration by using developer tools” on page 1556.

If you update the `bootstrap.properties` file, you must restart the server for the changes to take effect.

The `bootstrap.properties` file contains two types of properties:

- A small, predefined set of initialization properties.
- Any custom properties that you choose to define. You can then use these custom properties as variables in other configuration files such as `server.xml` and included files.

If you update the `bootstrap.properties` file, you must restart the server for the changes to take effect.

### Procedure

- Use predefined properties to configure trace and logging.

For example:

- To change the name of your trace file, specify the property `com.ibm.ws.logging.trace.file.name` with a file name of your choice, as follows:

```
com.ibm.ws.logging.trace.file.name = trace.log
```

- To enable binary logging, specify the `websphere.log.provider` property as follows:

```
websphere.log.provider = binaryLogging-1.0
```

For more information, see “Configuring binary logging in Liberty” on page 1031

- Use predefined properties for OSGi framework diagnostics. For example, set the port for the OSGi console as follows:

```
osgi.console = 5678
```

For more information, see “Using an OSGi console” on page 1587

- Use predefined properties for OSGi framework extensions. Specify the **org.osgi.framework.bootdelegation** if this property is required by external monitoring tools. The value is a comma-delimited list of packages.
- Use predefined properties for configuration password encryption. For more information, see “Liberty: The limits to protection through password encryption” on page 1009.
- Use custom properties to define the default ports for web applications.

You can share `server.xml` and use XML configuration files across various development environments that allow machine- or environment-specific customization. For example:

1. Specify the properties **default.http.port** and **default.https.port** in the `bootstrap.properties` file:

```
default.http.port = 9081
default.https.port = 9444
```

**Note:** If you do not specify the properties, the default HTTP port is 9080 and HTTPS ports is 9443. To override the default HTTP endpoint definition, set the `id` attribute of the `httpEndpoint` element to `defaultHttpEndpoint` in the server configuration.

2. Use the following properties in the `server.xml` configuration file:

```
<httpEndpoint id="defaultHttpEndpoint"
  host="*"
  httpPort="${default.http.port}"
  httpsPort="${default.https.port}" />
```

**Note:** `host="*"` means “listen on all adapters”. By default, the server is listening only on address `127.0.0.1/localhost`. You can also use the **host** property to specify a single IP address, and then the system listens only on the specified adapter.

- **8.5.5.2** Use custom properties to set the command port.

Set the command port to enable the server script to communicate with the running Liberty server and request certain operations, such as stopping the Liberty server or issuing a Java dump.

#### Distributed operating systems

IBM i

By default, the Liberty server acquires an ephemeral port to be used by the command listener. **z/OS** If you start the Liberty server from the shell script on z/OS, by default the Liberty server acquires an ephemeral port to be used by the command listener. If you start the Liberty server as a started task on z/OS, by default the command port is initially disabled, and all server administration tasks are accomplished by using `modify` commands that are issued to the z/OS operator console. These commands are described in *Administering Liberty on z/OS*. You can override the default behavior of the Liberty server by using the **command.port** property.

#### Valid values

- 1 Command port is disabled.
- 0 Ephemeral port is chosen at run time.
- 1-65535 User-specified port.

#### Default value

0 **Distributed operating systems** **IBM i** Ephemeral port is chosen at run time. **z/OS** If server is started from the shell script on z/OS, ephemeral port is chosen at run time.

**z/OS** -1

If server is started as a started task on z/OS, command port is disabled.

**Note:** **Distributed operating systems** **IBM i** You are discouraged from disabling the command port. If you disable the command port, you cannot use the server script to request some operations, for example, stopping the Liberty server or issuing a Java dump. **z/OS** You are discouraged from disabling the command port unless the server is running as a started task on z/OS. If you disable the command port, you cannot use the server script to request some operations, for example, stopping the Liberty server or issuing a Java dump.

- Use custom properties to configure server start wait time.

You can increase the server start wait time beyond the product default setting by adding the `server.start.wait.time` property to the `bootstrap.properties` file. The `server.start.wait.time` is specified in seconds.

1. Specify the `server.start.wait.time` property in the `bootstrap.properties` file. The following example sets the server start time to 25 seconds.

```
server.start.wait.time = 25
```

This setting means that as the server starts, the reporting mechanism for the server attempts to report on the completed stages of the start. If the reporting mechanism for the server cannot perform its function within 25 seconds, an error 22 occurs.

If you do not add the `server.start.wait.time` property to the `bootstrap.properties` file, the default server start wait time is internally set to 30 seconds.

- To apply the changes, restart the server.

---

## Setting the default host name of a Liberty server

### 8.5.5.0

You can add the `defaultHostName` variable to the `server.xml` file to set the default host name by which a Liberty server is identified.

### About this task

This variable is available for use by service configurations. Setting this value is particularly important for multihomed systems (with multiple NICs and multiple mapped host names for example).

#### Notes:

- This variable is currently used by the `<httpEndpoint>` `host` attribute and the `<hostAuthInfo>` `rpcHost` attribute
- The default host name should be the fully qualified host name of the system.
- The value should not contain any wildcards (\* for example).
- The variable default is `localhost`.

### Procedure

To set the default host name by which a Liberty server is identified, add the `defaultHostName` variable to the `server.xml` file.

For example:

```
<variable name="defaultHostName" value="localhost" />
```

## Liberty: Default port numbers

Some parts of Liberty use default TCP/IP port numbers. You can override the default port numbers by specifying a different port number in your server configuration.

### Runtime environment port numbers

For the command port, the Liberty server acquires an ephemeral port to be used by the command listener. You can configure this port in the `bootstrap.properties` file. For more information, see “Specifying Liberty bootstrap properties” on page 1437.

### Feature port numbers

The following table lists the default port numbers of Liberty features and an example of how you can override the default port in your server configuration.

Table 106. Default port numbers of Liberty features

Feature	Default port and configuration example
collectiveController-1.0	Replication port: 10010 <code>&lt;collectiveController   replicaPort="10012"/&gt;</code>  REST and JMX connections depend on the <code>restConnector-1.0</code> port.
8.5.5.6 <code>ejbRemote-3.2</code>	<ul style="list-style-type: none"><li>• IIOP port: 2809</li><li>• IIOP/SSL port: 9402</li></ul> <code>&lt;iiopEndpoint id="defaultIiopEndpoint" iiopPort="2809"&gt;   &lt;iioptionsOptions iiopsPort="9402" sslRef="defaultSSLConfig"/&gt; &lt;/iiopEndpoint&gt;</code>
8.5.5.7 <code>rtcomm-1.0</code>	<ul style="list-style-type: none"><li>• MQTT over TCP port: 1883</li><li>• MQTT over SSL port: 8883</li></ul> <code>&lt;mqtTtcpEndpoint id="defaultMqtTtcpEndpoint"   mqtTtcpPort="1885"   mqtTsslPort="8885"/&gt;</code>
<code>servlet-3.0</code>	<ul style="list-style-type: none"><li>• HTTP port: 9080</li><li>• HTTPS port: 9443</li></ul> <code>&lt;httpEndpoint id="defaultHttpEndpoint"   httpPort="9082"   httpsPort="9445" /&gt;</code>
8.5.5.7 <code>sipServlet-1.1</code>	<ul style="list-style-type: none"><li>• TCP port: 5060</li><li>• TLS port: 5061</li><li>• UDP port: 5060</li></ul> <code>&lt;sipEndpoint id="defaultSipEndpoint"   sipTCPport="5062"   sipUDPport="5062"   sipTLSport="5063" /&gt;</code>
<code>wasJmsServer-1.0</code>	<ul style="list-style-type: none"><li>• Incoming unsecure port: 7276</li><li>• Incoming secure port: 7286</li></ul> <code>&lt;wasJmsEndpoint id="InboundJmsEndpoint"   wasJmsPort="7278"   wasJmsSSLPort="7288"&gt; &lt;/wasJmsEndpoint&gt;</code>

---

## Using virtual hosts

8.5.5.7

You can use virtual hosts if you want isolation between applications and the endpoints that serve them.

A single application server is often responding to requests from multiple different host and port configurations. This occurs for a combination of reasons, such as it is running on a machine with multiple network interfaces with different names or it is routed to from an http server, proxy, or load balancer. In these cases, you might want to control which application can be contacted from a specific host. Virtual hosts provide this capability. It matches the requested host name and port number (as determined from the HTTP Host header) against the configured list of host aliases.

In WebSphere Application Server Liberty, the default configuration is sufficient. The default virtual host (default\_host) matches requests from any incoming host and port combination, and forwards them on to the default application container.

The following list illustrates the key configuration elements when you are configuring virtual hosts.

- The virtualHost configuration element ID value.
- The hostAlias subelement configuration.
- The allowFromEndpoint subelement configuration (if used).
- The virtual host configuration in the `ibm-web-bnd.xml` or `ibm-web-bnd.xmi` file of the WAR.
- The host attribute value of the `httpEndpoint`.
- The ID attribute value of the `httpEndpoint`.

### Isolating two applications from each other

The following example illustrates one of the more common usages of virtual hosting to give an understanding of some of the configuration that is required. This example shows how to configure two applications that run on differing ports. Further in this example illustrates that one application is only available on the localhost interface.

```
<httpEndpoint id="defaultHttpEndpoint" host="*" httpPort="9080" />
<httpEndpoint id="alternateEndpoint" host="*" httpPort="9081" />

<virtualHost id="application-1">
  <hostAlias>your_host_name:9080</hostAlias>
</virtualHost>

<virtualHost id="application-2">
  <hostAlias>localhost:9081</hostAlias>
</virtualHost>

<enterpriseApplication location="myApp.ear" name="App1"/>
<webApplication location="myApp2.war" name="App2" />
```

The `defaultHttpEndpoint` exposes all interfaces on port 9080, and the `alternateEndpoint` exposes all interfaces on port 9081.

If App1 has a WAR file with an `ibm-web-bnd.xml` file that specifies `<virtual-host name="application-1"/>`, then this application can be accessed only at `your_host_name:9080/app1_context_root`.

If App2 (which is a WAR) has an `ibm-web-bnd.xml` file that specifies `<virtual-host name="application-2"/>`, then this application can be accessed only at `localhost:9081/app2_context_root`.

If a third application was deployed which specified no specific virtual host, in this configuration, that application would be accessible only if it were a proxied request that contained HOST header that

specifies a different port. For example, if the request was made to a proxy on port 80, that port is not listed in any of the hostAlias specifications, and so the request would be routed to the default\_host virtual host.

## Isolating applications based on the requested host or port

The default virtual host in Liberty is also used for JMX communications. If you wanted to isolate JMX communications from application traffic, you would need to complete the following steps.

1. Decide on your virtual host name, and update your application to reference the new (non-default) host. Add a virtual-host element to the `ibm-web-bnd.xml` or `ibm-web-bnd.xmi` file of the WAR.

```
<?xml version="1.0" encoding="UTF-8"?>
<web-bnd
  xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xmk/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-web-bnd_1_0.x
  version="1.0" />

  <virtual-host name="proxiedRequests" />

</web-bnd>
```

2. Add a virtualHost element to your `server.xml` file. The name must match what is specified in the application, and must define hostAliases that are routed to the new virtual host.

**Note:** The host name and the port that is being matched is the one that is originally requested by the user, which might or might not match the host and port that Liberty is using. The following example illustrates a virtual host element added to your `server.xml` file.

```
<virtualHost id="proxiedRequests">
  <hostAlias>external.host.name:80</hostAlias>
  <hostAlias>external.host.name:443</hostAlias>
</virtualHost>
```

If requests are coming from a proxy, this configuration alone routes any request that is made to the proxy's host and port to the "proxiedRequests" virtual host.

## Restricting access based on originating endpoint

If you want to restrict access to the default/system applications that are using the defaultHttpEndpoint, there are more steps to take.

1. Define another httpEndpoint. The following example illustrates another httpEndpoint.

```
<httpEndpoint id="localhostOnly" host="localhost" httpPort="9081" httpsPort="9444"/>
```

This http endpoint specifies that `host="localhost"`, meaning that ports 9081 and 9444 are exposed only on the localhost interface.

2. Update virtualHost definitions to specify the `allowFromEndpointRef` attribute. When this attribute is specified, a virtualHost accepts requests only from the specified endpoint. For example:

```
<virtualHost id="default_host" allowFromEndpointRef="localhostOnly">
  <hostAlias>*:9081</hostAlias>
  <hostAlias>*:9444</hostAlias>
</virtualHost>

</virtualHost id="proxiedRequests">
  <hostAlias>*:9080</hostAlias>
  <hostAlias>*:9443</hostAlias>
  <hostAlias>external.host.name:80</hostAlias>
  <hostAlias>external.host.name:443</hostAlias>
</virtualHost>
```

With this configuration:

- The `default_host` virtual host now accepts requests that are directed only at `localhost:9081` and `localhost:9444` that also originate from the `localHostOnly` endpoint. Any other request to ports 9081 and 9444 are refused. For example, a request from the `defaultHttpEndpoint` with Host headers that reference `localhost:9081` is refused.
- The `proxiedRequests` virtual host now accepts any request that is issued to port 9080, or 9443 (which are the default ports that are used by the `defaultHttpEndpoint`), in addition to those that have a Host header that references the external host name from the proxy and port 80 or 443.

## Virtual hosts

8.5.5.7

A virtual host is a configuration entity that enables a single host machine to resemble multiple host machines.

A virtual host maintains a list of Multipurpose Internet Mail Extensions (MIME) types that it processes. You can associate a virtual host to one or more Web modules, but you can associate each web module with only one virtual host. Resources that are associated with one virtual host cannot share data with resources associated with another virtual host, even if the virtual hosts share a physical machine.

Each virtual host has a logical name and a list of one or more DNS aliases by which it is known. A DNS alias is the TCP/IP hostname and port number that is used to request the servlet, for example `yourHostName:80`. When no port number is specified, 80 is assumed.

The virtual host configuration uses wildcard entries with the ports for its virtual host entries.

- The default alias is `*:80` using an external port that is not secure.
- Aliases of the form `*:9080` use the internal port that is not secure.
- Aliases of the form `*:9443` use the secure internal port.
- Aliases of the form `*:443` use the secure external port.

A client request for a servlet, JavaServer Pages file, or related resource, contains a DNS alias and a Uniform Resource Indicator (URI) that is unique to that resource. When a client request for a servlet, JavaServer Pages file, or related resource is received, the DNS alias is compared to the list of all known virtual host groups to locate the correct virtual host. The URI is compared to the list of all known URI groups to locate the correct URI group. If the virtual host group and URI group are found, the request is sent to the corresponding server group for processing and a response is returned to browser. If a matching virtual host group or URI group is not found, an error is returned to the browser.

A virtual host is not associated with a particular node or machine. It is a configuration, rather than a live object, which is why you can create it, but cannot start or stop it. A default virtual host, named `default_host`, is automatically configured the first time that you start an application server. Unless you specifically want to isolate resources from one another on the same node, or physical machine, you probably do not need any virtual hosts in addition to the default host.

The DNS aliases for the default virtual host are configured as `*:80` and `*:9080`, where port 80 is the HTTP server port and port 9080 is the port for the default server's HTTP transport. The default virtual host includes common aliases, such as the machine's IP address, short host name, and fully qualified host name. One of these aliases comprises the first part of the path for accessing a resource such as a servlet. For example, the alias `localhost:80` is used in the request `http://localhost:80/myServlet`.

When you request a resource, the product tries to map the request to an alias of a defined virtual host. The `http://host:port/` portion of the virtual host is not case sensitive, but the URL that follows is case sensitive. The match for the URL must be alphanumerically exact. Different port numbers are treated as different aliases.

For example, the request `http://www.myhost.com/myservlet` maps successfully to `http://WWW.MYHOST.COM/myservlet` but not to `http://WWW.MYHOST.COM/MYSERVLET` or `Www.Myhost.Com/Myservlet`. In the latter two cases, these mappings fail because of case sensitivity. The request `http://www.myhost.com/myservletdoes` does not map successfully to `http://myhost/myservlet` or to `http://myhost:9876/myservlet`. These mappings fail because they are not alphanumerically correct.

You can use wildcard entries for aliases by port and specify that all valid host name and address combinations on a particular port map to a particular virtual host.

If you request a resource by using an alias that cannot be mapped to an alias of a defined virtual host, you receive a 404 error in the browser that you used to issue the request. A message states that the virtual host could not be found.

Two sets of associations occur for virtual hosts. Application deployment associates an application with a virtual host. Virtual host definitions associate the network address of the machine and the HTTP transport or web server port assignment of the application server with the virtual host. Looking at the flow from the web client request for the snoop servlet, for example, the following actions occur:

1. The web client asks for the snoop servlet: at web address `http://www.some_host.some_company.com:9080/snoop`
2. The `some_host` machine has the 9080 port that is assigned to the stand-alone application server, `server1`.
3. `Server1` looks at the virtual host assignments to determine the virtual host that is assigned to the alias `some_host.some_company.com:9080`.
4. The application server finds that no explicit alias for that DNS string exists. However, a wildcard assignment for host name `*` at port 9080 does exist, so this wildcard is a match. The virtual host that defines the match is `default_host`.
5. The application server looks at the applications that are deployed on the `default_host` and finds the snoop servlet.
6. The application server serves the application to the web client and the requester is able to use the snoop servlet.

*Table 107. Aliases for a virtual host*

Virtual host	Alias	Port number
default_host	*	9080
default_host	localhost	9080
default_host	my_machine	9080
default_host	my_machine.my_company.com	9080
default_host	localhost	80

You can have any number of aliases for a virtual host. You can even have overlapping aliases, such as:

The Application Server looks for a match by using the explicit address that is specified on the web client address. However, it might resolve the match to any other alias that matches the pattern before it matches the explicit address. Defining an alias first in the list of aliases does not guarantee the search order whenever the product is looking for a matching alias.

Virtual hosts with overlapping aliases. Assume that you define overlapping aliases for both virtual hosts because you accidentally defined port 9080 for the `admin_host` instead of port 9060:

A problem can occur if you use the same alias for two different virtual hosts. For example, assume that you installed the default application and the snoop servlet on the default\_host. You also have another virtual host that is called the admin\_host. However, you have not installed the default application or the snoop servlet on the admin\_host.

Table 108. Virtual hosts with overlapping aliases.

Virtual host	Alias	Port number
default_host	*	9080
default_host	localhost	9080
admin_host	*	9060
admin_host	my_machine.com	9080

Assume that a web client request comes in for `http://my_machine.com:9080/snoop`.

If the application server matches the request against `*:9080`, the application is served from the default\_host. If the application server matches the request to `my_machine.com:9080`, the application cannot be found. A 404 error occurs in the browser that issues the request. A message states that the virtual host could not be found.

This problem is the result of not finding the requested application in the first virtual host that has a matching alias. The correct way to code aliases is for the alias name on an incoming request to match only one virtual host in all of your virtual host definitions. If the URL can match more than one virtual host, you see the problem that is described.

---

## Preparing and running an application client

8.5.5.6

Learn how to prepare your server and client to run an application client from Liberty application client container.

### About this task

Running an application client successfully requires updates to both the `server.xml` and `client.xml` files.

### Procedure

Prepare your server, as follows:

1. Package a client module (`.jar`) and other modules, such as an EJB module (`.jar`), in an application EAR file.
2. Place the EAR file in the apps directory; for example, `wlp/usr/servers/your_server/apps`.
3. Update the `server.xml` configuration file by adding the `appClientSupport-1.0` feature, along with other necessary features.

**Important:** This step is not required if your application client is a stand-alone application.

4. Update the `server.xml` configuration file by configuring `<application/>` with your application information; for example:

```
<?xml version="1.0" encoding="UTF-8"?>
<server description="new server">
  <!-- Enable features -->
  <featureManager>
    <feature>javaee-7.0</feature>
  </featureManager>
  <application id="techsample" name="techSample" type="ear" location="TechnologySamples.ear"/>
</server>
```

Prepare your client, as follows:

5. Place the EAR file in the apps directory; for example, `wlp/usr/clients/your_client/apps`.
6. Update the `client.xml` configuration file by configuring `<application/>` with your application information; for example:

```
<?xml version="1.0" encoding="UTF-8"?>
<client description="new client">
  <!-- Enable features -->
  <featureManager>
    <feature>javaeeClient-7.0</feature>
  </featureManager>
  <application id="techsample" name="techSample" type="ear" location="TechnologySamples.ear"/>
</client>
```

7. Optional: Add the `appClientSecurity-1.0` feature to the `client.xml` file. Read about “Creating a Liberty application client manually.”
8. Start the server.
9. Run the client by entering `client run your_client`. If your client application uses command-line arguments, use the following format:  
`client run {your_client} -- arg1 arg2 ... argn`

There are additional steps to take if your server and client are running on different computers. By default, the server and client are using `localhost:2809`. You must configure IIOP to establish a connection between the server and client, as follows:

10. Stop the server.
11. Update the `server.xml` file with the IIOP configuration; for example:  
`<iiopEndpoint id="defaultIiopEndpoint" host="user.host.ibm.com" iiopPort="2814" />`
12. Update the `client.xml` file with the IIOP configuration; for example:  
`<orb id="defaultOrb" nameService="corbaname::user.host.ibm.com:2814" />`
13. Start the server.

## Creating a Liberty application client manually



8.5.5.6

You can create a Liberty application client from the command line.

### Before you begin

You enable the Java EE Application Client 7.0 feature in the `client.xml` file only.

### Procedure

1. Open a command line, then change directory to the `wlp/bin` directory. In the following examples, `path_to_liberty` specifies the location where you installed Liberty on your operating system.

**Windows** Example on Windows systems: `C:\Users\mo> cd path_to_liberty\wlp\bin`

**Linux** Example on Linux: `mo@machine01:~> cd path_to_liberty/wlp/bin`

2. Run the following command to create a client, where `client_name` is the name that you want to give your client. If you do not specify a client name, `defaultClient` is used.

**Windows** Example on Windows systems: `C:\wlp\bin> client create client_name`

**Linux** Example on Linux: `mo@machine01:~> client create client_name`

```
client create client_name
```

If the client is created successfully, you receive the following message:

```
Client client_name created.
```

You can find the `client.xml` file in the `wlp/usr/clients/client_name` directory. The file contains the `javaeeClient-7.0` feature.

**Attention:** If a default client exists, you get an error. If a default client does not exist, `defaultClient` is created.

3. Run your client application by preparing an application (`.ear`) file with a client module (`.jar`) in it. Specify a main class in the `MANIFEST.MF` of the client module, for example:

```
Manifest-Version: 1.0
Main-Class: com.ibm.ws.addressbook.ContactServiceClient_XMLInject
```

4. Place the EAR file under the `wlp/usr/clients/client_name/apps` directory.
5. Update the `client.xml` file to configure your application, for example:

```
<client>
  <featureManager>
    <feature>javaeeClient-7.0</feature>
  </featureManager>
  <application id="CLIENT_APP" name="CLIENT_APP" type="ear" location="clientApp.ear"/>
</client>
```

If the specified client already exists, no client is created and you receive an exception message:

```
CWWKE0005E: The runtime environment could not be launched.
CWWKE0904E: It was not possible to create the client called client_name because
the client directory C:\wlp\usr\clients\client_name already exists.
```

## What to do next

You can enable security (SSL, CSiv2, JAAS) for your application client by adding the `appSecurityClient-1.0` feature to your `client.xml` file:

```
<featureManager>
  <feature>javaeeClient-7.0</feature>
  <feature>appSecurityClient-1.0</feature>
</featureManager>
```

For more information about configuring security on the application client, see  [8.5.5.6](#) “Configuring security for the Liberty application client container and its applications” on page 1984.

## Creating a Liberty application client with multiple client modules

8.5.5.6

You can create a Liberty application client with multiple client modules in the same EAR file.

### About this task

You can specify more than one client application (packaged in a client module) in your application EAR file. If you would like to package multiple client applications in the same EAR file, you must use the `defaultClientModule` attribute in `<enterpriseApplication/>`.

### Procedure

Specify the client that you want to run by updating the `defaultClientModule` attribute in both the `client.xml` and `server.xml` files.

```
<client>
  <featureManager>
    <feature>javaeeClient-7.0</feature>
  </featureManager>
  <enterpriseApplication id="MultipleAppClientModules" name="MultipleAppClientModules" type="ear"
    defaultClientModule="HelloAppClient.jar" location="MultipleAppClientModules.ear"/>
</client>
```

**Important:** You can run one application at a time.

---

## Setting up the server-management environment for Liberty by using collectives

### 8.5.5.0

To set up the server-management environment for Liberty by using collectives, define the appropriate features in the `server.xml` file and run the corresponding collective command-line tasks to establish the administrative domain security configuration.

### About this task

You can use collectives to manage multiple servers from a single management domain. For high availability, you can configure collective replica sets, clusters, or scaling. For general information about collectives, see “Liberty: Collective architecture” on page 1450.

Liberty provides multiple-server management in the following features:

- **collectiveController-1.0**

The `collectiveController-1.0` feature enables controller functionality for a management collective and includes collective- and cluster-management MBeans that are accessible using the REST JMX connector that is provided by the `restConnector-1.0` feature. The collective controller acts as a storage and collaboration mechanism to which collective members can connect. The administrative domain security configuration for the `collectiveController-1.0` feature is established using the **collective** command-line **create** and **replicate** tasks.

**Distributed operating systems**

IBM i

The `collectiveController-1.0` feature and its capabilities are available only in multiple-server products such as WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in single-server products such as WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a multiple-server product installation, you can use its `collectiveController-1.0` feature to work with collective members from single-server products.

- **collectiveMember-1.0**

The `collectiveMember-1.0` feature enables a server to be a member of a management collective and be managed by the collective controller. The administrative domain security configuration for the `collectiveMember-1.0` feature is established using the **collective** command-line **join** task.

**Tip:** All servers enabled with the `collectiveController-1.0` feature are managed; therefore, you do not need to specify `collectiveMember-1.0` if the server already has the `collectiveController-1.0` feature enabled.

- **clusterMember-1.0**

The cluster member feature enables a collective member to participate in a static cluster.

8.5.5.4

- **dynamicRouting-1.0**

The dynamic routing feature is an Intelligent Management feature of the WebSphere plug-in for Apache and IHS that provides On Demand Router capabilities for the plug-in. The dynamic routing feature enables a server to run a REST service to which the plug-in can connect in order to dynamically route to all servers in a collective.

8.5.5.4

- **scalingController-1.0**

The scaling controller feature enables a collective controller to expand or contract an auto scaling cluster and manage the scaling controller. If an environment has many scaling controllers, only one of the running scaling controllers can make decisions. If that controller is stopped, another running

scaling controller takes over for it. The scaling controller can start an auto scaling cluster member in response to increased resource usage, or it might stop an auto scaling cluster member in response to decreased resource usage.

- **8.5.5.4 scalingMember-1.0**

The scaling member feature monitors the workload within a server and its host, then sends this information to the scaling controller. The scaling controller feature is enabled in the collective controllers that are part of the collective. This feature also enables dynamic clustering of the collective members and allows the servers to dynamically start or stop based on criteria that is specified by the scaling policy. If more than one scaling member is on the same host, each scaling member must define a `hostSingleton` element with a port in the `server.xml` file. All scaling members on the same host must use the same port to identify a host leader. The host leader is the only scaling member that communicates with the scaling controller. It communicates metric data from the members to the controller and communicates scaling decisions that are made by the controller to the members in the host.

## Procedure

- Configure a server to act as collective controller.
  - Create a collective controller server using commands and then configure the controller `server.xml` file. See step 1 of “Configuring a Liberty collective” on page 1136.
  - Create a collective controller using developer tools. See step 1 of “Configuring a Liberty collective using the developer tools” on page 1460.
- Join a server to a collective as a member.
  - Join a server to a collective using commands and then configure the member `server.xml` file. See step 2 of “Configuring a Liberty collective” on page 1136.
  - Join a server to a collective using developer tools. See step 2 of “Configuring a Liberty collective using the developer tools” on page 1460.
- Change the collective configuration as needed for your environment.
  - Register host computers with a collective.
  - Override host information by revising parameters in the `hostAuthInfo` element of the member `server.xml` file.
  - Set up Remote Execution and Access (RXA) to enable collective controllers to start and stop servers.
  - Set the `JAVA_HOME` variable for Liberty collective members.
  - Generate collective controller SSL keys.
  - **8.5.5.5** Set administrative metadata for Liberty resources in an `admin-metadata.xml` file.
- Create a replica set, which is a set of collective controllers that are configured to work together, to provide management high availability.
  - **8.5.5.5** Automatically share configurations among replicas.
  - **8.5.5.7** Change the port of a replica.
- Backup, upgrade, or remove a collective controller, replica set, or member.
- Set up static cluster members to provide application high availability and scale.
- **Distributed operating systems** **z/OS** Set up dynamic routing of HTTP requests to collective members.
- **Distributed operating systems** **z/OS** **8.5.5.4** Set up autonomic scaling of collectives.
  - Set up auto scaling for use with Intelligent Management dynamic routing.
  - Configure auto-scalable clusters for JVM elasticity.
  - **8.5.5.7** Configure provisionable clusters for Liberty elasticity.
  - Define scaling policies.
  - **8.5.5.5** Set scaling policies for an auto-scalable cluster in a `scaling-metadata.xml` file.
- **8.5.5.7** Enter maintenance mode before you perform diagnostic tests, maintenance, or tuning on a host or server.
- **8.5.5.7** Configure health management to prevent disruption of service by detecting common problems and generating diagnostic actions based on configured health policies.

## What to do next

You can administer the collective using the following tools:

- Use Jython scripts or a Java client such as JConsole to perform collective controller MBean operations.
- Run collective commands from a command line at the bin directory of your Liberty installation. For information about collective commands, run the collective **help** command:

```
wlp/bin/collective help
```

To view details about a specific command, include the command name; for example, to view details about the collective **create** command, run:

```
wlp/bin/collective help create
```

**Tip:** The example commands in this documentation are prefaced with `wlp/bin/`. This means to open a command line at the `bin` directory of your Liberty installation, such as `C:\wlp\bin` on Windows operating systems, and run the command.

- **8.5.5.2** Use WebSphere Liberty Administrative Center ("Admin Center") to administer Liberty servers, applications, and other resources in the collective from a web browser on a smartphone, tablet, or computer.
  1. Add the `adminCenter-1.0` feature to the collective controller `server.xml` file.
  2. To access Admin Center from a smartphone, tablet, or remote computer, ensure that the `server.xml` file sets the `host` attribute of the `httpEndpoint` element to `*` (asterisk) or to a defined host name.
  3. Point a web browser at Admin Center. The URL uses the form:  
`https://collective_controller_host_name:collective_controller_port/adminCenter/`
  4. If your browser prompts you to confirm that the connection is trusted, specify an exception or otherwise enable the connection to continue to Admin Center.
  5. Log in using your collective controller administrative user name and password.
  6. From the Toolbox, open the Server Config tool or Explore tool.
    - **8.5.5.7** Select . Use the Server Config tool to view and edit server configuration files such as `server.xml` files in the collective. For information about the Server Config tool, see "Editing server configuration files in Admin Center" on page 1748.
    - **8.5.5.5** Select . Use the Explore tool to manage applications, clusters, servers, and hosts in the collective. For information about the Explore tool, see "Exploring and managing resources with Admin Center" on page 1749.

For other information about enabling and using Admin Center, see "Administering Liberty using Admin Center" on page 1741.

To ensure that you can remotely start and stop servers, complete the steps for your operating system in "Setting up RXA for Liberty collective operations" on page 1491.

## Liberty: Collective architecture

The set of Liberty servers in a single management domain is called a *collective*. A collective consists of at least one server with the `collectiveController-1.0` feature enabled that is called a *collective controller*. Optionally, a collective can have many servers with the `collectiveMember-1.0` feature enabled that are called *collective members* and a collective can be configured to have many collective controllers.

**Note:** **Distributed operating systems**  The `collectiveController-1.0` feature and its capabilities are available only in multiple-server products such as WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in single-server products such as WebSphere Application Server Liberty or WebSphere Application Server Liberty Core. If you have a multiple-server product installation, you can use its `collectiveController-1.0` feature to work with collective members from single-server products.

The collective controller provides for a centralized administrative control point to perform operations such as MBean routing, file transfer, and cluster management. A core role of collective controllers is to receive information, such as MBean attributes and operational state, from the members within the collective so that the data can be retrieved readily without having to invoke an operation on each individual member.

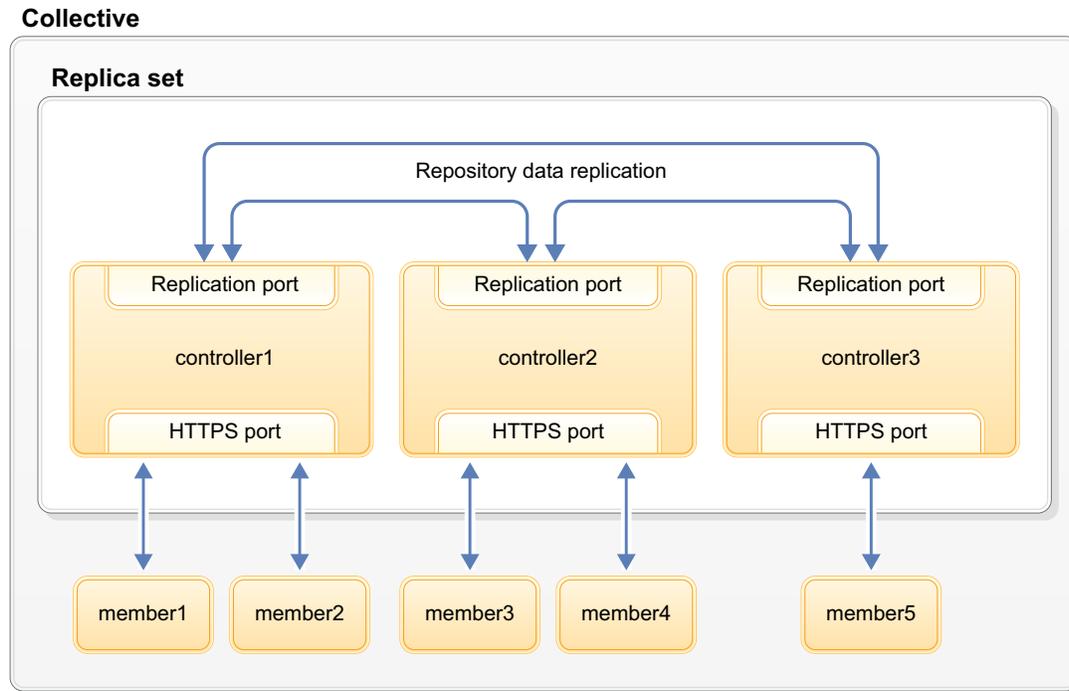


Figure 23. Liberty collective architecture

A set of collective controllers is called a *replica set*. There is only one replica set per collective, and all controllers must be part of the replica set. When there is more than one collective controller, each collective controller replicates its data to the other collective controllers in the replica set to allow for high availability and data protection. The replica set is logically present even when only one controller is in use. When changing your configuration to multiple replicas in a set, include at least three replicas in the set. The controllers in the replica set communicate with each other using a collaboration scheme to ensure that data is replicated across the set of controllers no matter which controller in the set receives an operation to store data. Each controller has a dedicated port for use by the replication protocol. Communication between the controllers in the replica set is always authenticated and protected with SSL.

A collective member can be configured with multiple collective controller endpoints. A collective member only communicates with one collective controller at a time; however, a configuration with more than one collective controller endpoint provides failover and workload balancing. Member-to-controller communication is always in the form of MBean operations that are performed over the IBM JMX Rest Connector. Communication between controllers and members is always authenticated and protected with SSL.

See “Setting up the server-management environment for Liberty by using collectives” on page 1134 for more information.

#### Administrative domain security configuration:

The administrative domain security configuration is made up of two parts:

- User domain

This domain relies on Java role-based security that defines the Administrator role. This can be mapped to users within the configured user registry.

- Server domain

This domain relies on SSL certificate-based authentication.

For more on collective security, see “Liberty: Collective security” on page 1453.

## Configured and standby replicas

Replicas that have been added to a configured replica set are running (*active replicas*) or stopped (*inactive replicas*). A replica that is started and that has never been added to a configured replica set, or was removed from a configured replica set, is called a *standby replica*.

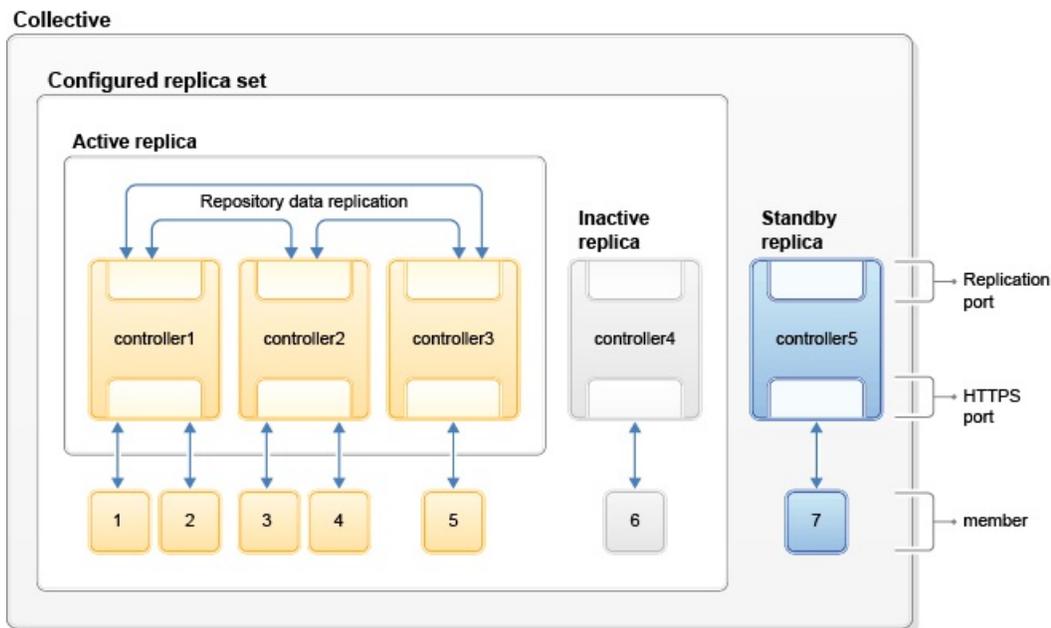


Figure 24. Configured and standby replicas in a collective controller

## Summary of collective architecture terms

### collective

The set of Liberty servers in a single management domain.

### collective controller

A server that has the `collectiveController-1.0` feature enabled.

### collective member

A server that has the `collectiveMember-1.0` feature enabled.

### replica set

A set of collective controllers. For optimal functionality and high availability, a replica set must have at least three controllers.

### replica port

A dedicated port on a controller that is used by the replication protocol.

### configured replica set

The union of the active replicas and inactive replicas.

### active replicas

The started replicas that have been added to the configured replica set.

### inactive replicas

The stopped replicas that have been added to the configured replica set.

### standby replica

The started replicas that have not been added to the configured replica set or that were removed from the configured replica set.

## Liberty: Collective security

8.5.5.0

You can use the principles of collective security in Liberty to address data in motion and data at rest.

The two principal areas of collective security are:

- Administrative domain security configuration  
Addresses data in motion, authentication and authorization
- Collective repository data security  
Addresses data at rest, authentication and authorization

### Administrative domain security configuration

The administrative domain security configuration for collectives is comprised of two parts:

- User domain  
This domain relies on Java role-based security that defines the Administrator role. This can be mapped to users within the configured user registry.
- Server domain  
This domain relies on SSL certificate-based authentication.

In order for users to access the collective controller's MBeans, they must be in the Administrator role. All administrative actions through the collective require that the user be granted the Administrator role. See “Configuring secure JMX connection to Liberty” on page 1642 for complete details.

Server-to-server communication falls within the server domain and no user identities or passwords are used to communicate between members of a collective. Each member of the collective has a unique identity within the collective that is comprised of its host name, user directory, and server name. Each member within the collective defines its server domain configuration, which consists of the `serverIdentity.jks` and `collectiveTrust.jks` files. These files contain the SSL certificates that are necessary to establish secure communications within the collective. The HTTPS key configuration must have specific trust settings, which are established by default.

The server domain SSL configuration can be customized by adding additional trusted certificate entries to the `collectiveTrust.jks` keystore. All trust is copied when a controller is replicated; therefore, SSL customization should be applied to the initial controller. Adding trust to the `collectiveTrust.jks` keystore is only necessary if the default HTTPS certificates are not used. If the HTTPS SSL configuration is modified, the following certificate rules apply:

- HTTPS trust must be established by all controllers and members within the collective. If the HTTPS SSL certificates are modified, the following root signers from the collective controller must be added to the HTTPS SSL truststore:
  - The `controllerRoot` signer from the `rootKeys.jks` keystore must be added to all collective members HTTPS SSL truststore.
  - The `controllerRoot` signer and the `memberRoot` signer from the `rootKeys.jks` keystore must be added to all collective controllers' HTTPS SSL truststore.
- Each member can make an outbound connection to a collective controller. The collective controller's `collectiveTrust.jks` keystore must contain a certificate chain that trusts the

HTTPS SSL certificate for each member. It is highly recommended that all HTTPS certificates be signed by a root signer, which then can be added to the `collectiveTrust.jks` keystore. Using individual SSL certificates that do not have a common root signer is sufficient to establish trust but will not scale.

- Each controller can make an outbound connection to a collective member. The collective member's `collectiveTrust.jks` keystore must contain a certificate chain that trusts the HTTPS SSL certificate for each controller. It is highly recommended that all HTTPS certificates be signed by a root signer, which then can be added to the `collectiveTrust.jks` keystore. Using individual SSL certificates that do not have a common root signer is sufficient to establish trust but will not scale.

Server-to-server communication requires that SSL authentication be supported. If the HTTPS SSL configuration is customized, the SSL configuration must specify `clientAuthenticationSupported="true"`. For example:

```
<!-- clientAuthenticationSupported set to enable bidirectional trust -->
  <ssl id="defaultSSLConfig"
    keyStoreRef="defaultKeyStore"
    trustStoreRef="defaultTrustStore"
    clientAuthenticationSupported="true" />
```

Setting `clientAuthentication="true"` on the collective controller is inadvisable and prevents some common and expected behaviors. For example, this setting prevents authentication with user names and passwords in Admin Center and collective command line utilities.

Setting `clientAuthentication="true"` on a collective member might be desirable to prevent user name and password logins. This setting does not break collective operations as all operations originating from the controller are authenticated using the certificate.

Members can be prevented from publishing information to the collective controller by using the `CollectiveRegistration` MBean. The `disavow` and `avow` methods prevent authentication and enable authentication.

### Collective repository data security

The collective repository data security policy covers the policy for data at rest - specifically, the policy of accessing the contents of the collective repository.

The current security policy for collective data is as follows:

- The system reserves three node names: `sys.host.auth.info`, `sys.jmx.auth.info`, and `sys.nologin`. These nodes are under a host or server's repository namespace. User-created nodes should avoid using the `sys.` prefix.
- The `sys.host.auth.info` and `sys.jmx.auth.info` nodes are not accessible through the MBean to prevent disclosure of system credentials. Accessing the data stored at these nodes will result in a null response.
- A collective member is restricted to modifying only its own information in the repository. Authenticated administrative users have unrestricted access to information in the repository except as previously noted. Authenticated administrative users are all users granted the Administrative role.

Because the collective repository ultimately resides on the disk, the file system permission settings must be secure for the environment. It is recommended that the collective controller's configuration be readable and writable only by the user, readable only by the group, and not accessible at all by the world - in other words, `chmod 0640`. Follow any security guidelines that your organization might have established.

## Configuring a Liberty collective

You can organize Liberty servers into collectives to support clustering, administration, and other operations that act on multiple Liberty servers. By using collectives, you can efficiently and accurately deliver application services to your organization.

## Before you begin

The `collectiveController-1.0` feature and its capabilities are available only in WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a WebSphere Application Server Liberty Network Deployment installation, you can use its `collectiveController-1.0` feature to work with collective members from WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core installations.

## About this task

A Liberty collective is a set of Liberty servers that are configured as part of the same administrative and operational domain.

Configuration and state data about a Liberty collective is housed in an active operational repository.

Membership in a Liberty collective is optional. Liberty servers join a collective by registering with a collective controller to become members. Members share information about themselves through the operational repository of the controller.

The following rules apply:

- A Liberty server can be a member of only one collective.
- Different Liberty servers on the same host can be in different collectives.
- Liberty servers on the same host that are members of a collective can coexist with Liberty servers that are not members of a collective.

 **Watch:** Introduction to creating a collective demonstrates the procedure. This video, and other information about collectives, is available on the WASdev website. [Transcript]

## Procedure

1. Create and configure your controller.
  - a. Create a server to act as the collective controller.

```
wlp/bin/server create myController
```

- b. Create the collective controller configuration.

The collective controller configuration consists primarily of the administrative domain security configuration that is used for secure communication between controllers and members.

```
wlp/bin/collective create myController --keystorePassword=controllerKSPassword
```

**8.5.5.2** By default, this collective command writes all output to a console screen. In the next step, you copy the configuration output into the `server.xml`. To write the configuration to a file instead of to a console screen, specify a `--createConfigFile=outputFilePath` parameter, for example:

```
wlp/bin/collective create myController --keystorePassword=controllerKSPassword --createConfigFile=c:\wlp\usr\servers\myController\
```

After you run the **create** command, the `include` statement to use is displayed. To include the outputted file in the collective configuration, add the `include` statement to the `server.xml` file, for example:

```
<include location="c:\wlp\usr\servers\myController\collective-create-include.xml" />
```

- c. Update the `server.xml` file of the collective controller.

- Copy and paste output.

If the command wrote output to a console screen, proceed with the following steps:

- 1) Copy output from the collective command and paste it into the server.xml file.
- 2) Specify administrative user ID and password values for the collective. For example, change:

```
<quickStartSecurity userName="" userPassword="" />
```

to:

```
<quickStartSecurity userName="adminUser" userPassword="adminPassword" />
```

The default path for the collective controller server.xml file is `${wlp.install.dir}/usr/servers/myController/server.xml` or, if the `$WLP_USER_DIR` variable is set in a server.env file or command window, `$WLP_USER_DIR/servers/myController/server.xml`. After editing, the file will resemble the following example:

```
<server description="controller server">
  <!-- Enable features -->
  <featureManager>
    <feature>jsp-2.2</feature>
  </featureManager>
  <httpEndpoint id="defaultHttpEndpoint"
    host="*"
    httpPort="9080"
    httpsPort="9443" />
  <featureManager>
    <feature>collectiveController-1.0</feature>
  </featureManager>
  <!-- Define the host name for use by the collective.
  If the host name needs to be changed, the server should be
  removed from the collective and re-joined or re-replicated. -->
  <variable name="defaultHostName" value="controllerHostname" />
  <!-- TODO: Set the security configuration for Administrative access -->
  <quickStartSecurity userName="adminUser" userPassword="adminPassword" />
  <!-- clientAuthenticationSupported set to enable bidirectional trust -->
  <ssl id="defaultSSLConfig"
    keyStoreRef="defaultKeyStore"
    trustStoreRef="defaultTrustStore"
    clientAuthenticationSupported="true" />
  <!-- inbound (HTTPS) keystore -->
  <keyStore id="defaultKeyStore" password="yourPassword"
    location="${server.config.dir}/resources/security/key.jks" />
  <!-- inbound (HTTPS) truststore -->
  <keyStore id="defaultTrustStore" password="yourPassword"
    location="${server.config.dir}/resources/security/trust.jks" />
  <!-- server identity keystore -->
  <keyStore id="serverIdentity" password="yourPassword"
    location="${server.config.dir}/resources/collective/serverIdentity.jks" />
  <!-- collective trust keystore -->
  <keyStore id="collectiveTrust" password="yourPassword"
    location="${server.config.dir}/resources/collective/collectiveTrust.jks" />
  <!-- collective root signers keystore -->
  <keyStore id="collectiveRootKeys" password="yourPassword"
    location="${server.config.dir}/resources/collective/rootKeys.jks" />
</server>
```

- **8.5.5.2** Add an include statement.

If you wrote the output to a file by using the `--createConfigFile=outputFilePath` parameter, add an include statement to `$WLP_USER_DIR/servers/myController/server.xml` to include the outputted file in the collective configuration. For example:

```

<server description="controller server">
  <!-- Enable features -->
  <featureManager>
    <feature>jsp-2.2</feature>
  </featureManager>
  <httpEndpoint id="defaultHttpEndpoint"
    host="*"
    httpPort="9080"
    httpsPort="9443" />
  <include location="c:\wlp\usr\servers\myController\collective-create-include.xml" />
</server>

```

Ensure the outputted file sets administrative user ID and password values for the collective, for example:

```
<quickStartSecurity userName="adminUser" userPassword="adminPassword" />
```

d. Start the collective controller server.

```
wlp/bin/server start myController
```



Figure 25. Collective of one

e. Verify that the collective controller server started correctly and is ready to receive members.

- 1) Open an editor on the collective controller messages log, \$WLP\_USER\_DIR/servers/myController/logs/messages.log.
- 2) Look for the following message:

```
CWWKX9003I: CollectiveRegistration MBean is available.
```

```

| If you want to enable a collective controller and its members to use the security TLSv1.2 protocol
| for the Secure Sockets Layer (SSL) context, see "Setting up Liberty to run in SP800-131a" on page
| 1848. The server.xml files of the controller and members need ssl id elements and each host
| computer needs a server.env file with the JVM_ARGS=-Dhttps.protocols=TLSv1.2 statement in its
| ${wlp.install.dir}/etc directory.

```

2. Create and configure a member to join the collective.

The controller and members can be on separate hosts. In this example, the controller and member are on the same host.

a. Create a member server.

```
wlp/bin/server create myMember
```

b. Join the member.

Run the collective **join** command to join the server to the collective as a member.

The **join** command requires a network connection to the collective controller and an administrative user ID and password for performing MBean operations on the controller. Look at the server.xml file of the collective controller to find the values for the --host, --port, --user, and --password parameters. For --keystorePassword, set a value to use for the member keystore password, such as memberKSPassword. You can specify different --keystorePassword values for each server that is joined to the collective.

```
wlp/bin/collective join myMember --host=controllerHostname --port=9443 --user=adminUser --password=adminPassword --keystorePassword=memberKSPassword
```

The optional parameter --hostname specifies the host name to use for the system. Set --hostname only if the system has multiple host names or does not have its host name configured. If set, the value must match the defaultHostName variable that is defined in the server.xml file.

**8.5.5.2** To write the output of this collective command to a file, instead of to a console screen, specify an optional `--createConfigFile=outputFilePath` parameter. Then, include the outputted file in the collective configuration by adding an `include` statement to the member `server.xml` file:

**8.5.5.2**

```
<include location=outputFilePath />
```

**8.5.5.4** By default, the **join** operation leaves remote procedure call (RPC) credentials undefined. You must specify values for `rpcUser`, `rpcUserPassword`, and the operating system login user and password for the host on which the member server resides. If the member host is registered with the collective controller and the member host is not enabled for SSH, specify an optional `--useHostCredentials` parameter to enable the member to inherit RPC credentials from its host registration on the controller. Typically, Linux hosts are enabled for SSH and Windows hosts are not enabled for SSH; thus, the `--useHostCredentials` parameter is useful for Windows member hosts. Specifying `--useHostCredentials` adds `<hostAuthInfo useHostCredentials="true" />` to the member `server.xml` file. You then can run collective member server commands such as **start** or **stop** without specifying RPC credentials because the member inherits credentials from its host. See “Overriding Liberty server host information” on page 1144 for information about `hostAuthInfo`, the `--useHostCredentials` parameter, and connecting the collective controller to the server.

For information about these required parameters and about optional parameters, run `collective help join` at a command line.

- c. If prompted to accept the certificate chain, enter `y` (yes).
- d. Update the member `server.xml` file.
  - Copy and paste output.

If the command wrote output to a console screen, proceed with the following steps:

- 1) Copy output from the collective command and paste it into the member `server.xml` file.
- 2) Modify the ports so that the server can open its HTTP ports. Ensure the member `server.xml` sets unique HTTP port numbers on its host. For example, if the member is on the same host as the collective controller, change the HTTP port numbers:

```
<httpEndpoint id="defaultHttpEndpoint" httpPort="9081" httpsPort="9444" />
```

Optionally, to access the member server from a remote client, also set `host="*"` in the `httpEndpoint` element.

In `$WLP_USER_DIR/servers/myMember/server.xml`, for example:

```
<server description="member server">
  <!-- Enable features -->
  <featureManager>
    <feature>jsp-2.2</feature>
  </featureManager>
  <httpEndpoint id="defaultHttpEndpoint"
    host="*"
    httpPort="9081"
    httpsPort="9444" />
  <featureManager>
    <feature>collectiveMember-1.0</feature>
  </featureManager>
  <!-- Define the host name for use by the collective.
  If the host name needs to be changed, the server should be
  removed from the collective and re-joined or re-replicated. -->
  <variable name="defaultHostName" value="memberHostname" />
```

**8.5.5.4** `<!-- Remote host authentication configuration --> <hostAuthInfo rpcUser="admin_user_id" rpcUserPassword="admin_user_password" /> <!-- Connection to the`

```

collective controller --> <collectiveMember controllerHost="controllerHostname"
controllerPort="9443" /> <!-- clientAuthenticationSupported set to enable bidirectional trust -->
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore" trustStoreRef="defaultTrustStore"
clientAuthenticationSupported="true" /> <!-- inbound (HTTPS) keystore --> <keyStore
id="defaultKeyStore" password="yourPassword" location="{server.config.dir}/resources/
security/key.jks" /> <!-- inbound (HTTPS) truststore --> <keyStore id="defaultTrustStore"
password="yourPassword" location="{server.config.dir}/resources/security/trust.jks" /> <!--
server identity keystore --> <keyStore id="serverIdentity" password="yourPassword"
location="{server.config.dir}/resources/collective/serverIdentity.jks" /> <!-- collective truststore
--> <keyStore id="collectiveTrust" password="yourPassword" location="{server.config.dir}/
resources/collective/collectiveTrust.jks" /> </server>

```

- **8.5.5.2** Add an include statement.

If you wrote the output to a file by using the `--createConfigFile=outputFilePath` parameter, add an include statement to `$WLP_USER_DIR/servers/myMember/server.xml` to include the outputted file, for example:

```

<server description="member server">
    <!-- Enable features -->

    <featureManager>
        <feature>jsp-2.2</feature>
    </featureManager>

    <httpEndpoint id="defaultHttpEndpoint"
        host="*"
        httpPort="9081"
        httpsPort="9444" />

    <include location="c:\wlp\usr\servers\myMember\collective-join-include.xml" />
</server>

```

- e. **8.5.5.4** If you did not specify `--useHostCredentials` in the `join` command and the member host is not enabled for SSH, set RPC credentials for `hostAuthInfo` in the member `server.xml` file or the outputted file. You can set RPC credentials for the member server in either of two ways:

- Set `hostAuthInfo` RPC user and password values. Set `rpcUser` to an operating system login user ID for the host on which the member server resides, and set `rpcUserPassword` to the operating system login password for the user ID. For example, if you log into the member computer with user `test1` and password `test1pwd`, then change the `hostAuthInfo` element to the following:

```
<hostAuthInfo rpcUser="test1" rpcUserPassword="test1pwd" />
```

- If the member host is registered with the collective controller, set `hostAuthInfo useHostCredentials` to `true` for the member server to inherit RPC credentials from its host.

```
<hostAuthInfo useHostCredentials="true" />
```

See “Overriding Liberty server host information” on page 1144 for information about `hostAuthInfo` settings and for an example that shows how to register a member host and run the `join` command with `--useHostCredentials`.

- f. **z/OS** For z/OS only, issue the `updateHost` command to specify the member `JAVA_HOME` directory for the controller.

```

collective updateHost controllerHostname --host=controllerHostname
--port=9443 --user=adminUser --password=adminPassword
--hostWritePath=/dir1 --rpcUser=rpcUser
--rpcUserPassword=rpcUserPassword --hostJavaHome=JAVA_HOME

```

The `hostWritePath` parameter specifies the directories to which the collective controller can write. Paths that are specified by the `hostWritePath` parameter are also readable.

The `hostJavaHome` parameter specifies the absolute path to where the JVM is on the system and where the member server runs, for example `/usr/lpp/java/java_1.7_64`

- g. Start the member server.

```
wlp/bin/server start myMember
```

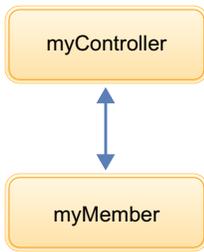


Figure 26. Simple collective

- h. Verify that the member server started correctly and is publishing information to the controller.
  - 1) Open an editor on the member messages log, `$WLP_USER_DIR/servers/myMember/logs/messages.log`.
  - 2) Look for the following messages in any order:
 

```

CWWKX8112I: The server's host information was successfully published to the collective repository.
CWWKX8114I: The server's paths were successfully published to the collective repository.
CWWKX8116I: The server STARTED state was successfully published to the collective repository.
          
```

## Configuring a Liberty collective using the developer tools

### 8.5.5.1

Using the Liberty **Utilities** menu in the developer tools, you can create a collective controller or join a collective.

### Before you begin

Using the developer tools simplifies the process of configuring a Liberty collective by providing convenient utilities for creating collective controllers or joining collectives. For more information about Liberty collectives, see “Configuring a Liberty collective” on page 1136.

### Procedure

1. Creating a collective controller:

**Note:** Creating a collective controller can be done only with the following editions:

- WebSphere Application Server Liberty Network Deployment
  - WebSphere Application Server Liberty for z/OS
- a. In the Servers view, right-click your Liberty server, and select **Utilities > Create Collective Controller**.
  - b. In the **Keystore password** field, type a password for your collective.
  - c. Click **Finish**.

Results:

An information dialog appears after the collective configuration is complete. This dialog informs you that the `server.xml` file was already updated to include the generated configuration file. If there are instructions to add the configuration lines to the `server.xml` in the console output, they can be ignored. However, Administrative Security and other settings might still need to be configured within the included configuration file before any collective members can join.

2. Joining a collective controller:

**Note:** You must have a collective controller available before a server can be added to a collective. Joining a collective can be done with the following editions:

- WebSphere Application Server Liberty

- WebSphere Application Server Liberty - Express
- WebSphere Application Server Liberty Core

  - a. In the Servers view, right-click your Liberty server, and select **Utilities > Join Collective**.
  - b. On the Join Collective page, specify the information of the collective controller you would like to join.
  - c. In the **Host** field, type in the host name for the collective controller.
  - d. In the **Port** field, type in the port number for the collective controller.
  - e. In the **User** field, type in the user name for the collective controller.
  - f. In the **Password** field, type in the password for the collective controller.
  - g. In the **Keystore password** field, type the keystore password for the collective controller if encryption was used.
  - h. Click **Finish**.

Results:

An information dialog appears after the collective configuration is complete. This dialog informs you that the `server.xml` file was already updated to include the generated configuration file. If there are instructions to add the configuration lines to the `server.xml` in the console output, they can be ignored.

## Overriding Liberty server host information

### 8.5.5.0

The `collectiveMember-1.0` feature enables a server to be managed by the collective controller. Most server host information can be automatically detected. In certain scenarios, however, you must provide additional host information so that the collective controller can establish a connection to the server.

**Note:** **Distributed operating systems** **IBM i** The `collectiveController-1.0` feature and its capabilities are available only in WebSphere Application Server Liberty Network Deployment and WebSphere

Application Server Liberty for z/OS. **8.5.5.0** The feature is not available in WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a WebSphere Application Server Liberty Network Deployment installation, you can use its `collectiveController-1.0` feature to work with collective members from WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core installations.

To enable the host information override, add the following element to the `server.xml` file:

```
<hostAuthInfo rpcPort="ssh_port"
  rpcUser="user_ID"
  rpcUserPassword="password"
  rpcUserHome="user_home"
  rpcHost="host_name"
  sudoUser="sudo_user"
  sudoPassword="sudo_user_password"
  sshPublicKeyPath="public_key_path"
  sshPrivateKeyPath="private_key_path"
  sshPrivateKeyPassword="private_key_password"
```

**8.5.5.4** `useHostCredentials="true_or_false"/>`

#### **rpcPort**

This parameter specifies the port for the RPC mechanism, which is SSH port 22 by default. If your system uses a nonstandard port, set this value accordingly. If this value is not specified, the default value is 22.

### **rpcUser**

This parameter specifies the user ID that the collective controller will use to connect to the server. If the host does not support SSH or using SSH keys is not desired, you can use this parameter to specify an operating system login user. For example, if you log in to the host with the myID user, then you specify `rpcUser="myID"`. If this value is not specified, the default value is `System.getProperty("user.name")`.

### **rpcUserPassword**

This parameter specifies the password for the specified user ID. For example, if you log in to the host with the myID user and the myPwd password, then you specify `rpcUser="myID"` and `rpcUserPassword="myPwd"`. If this value is not specified, the server will either generate an SSH key pair or use the SSH key pair for the connection that is specified using the **privateKeyPath** and **publicKeyPath** parameters. If SSH is not installed on the server (such as on a Windows or OS/400 operating system), the password is required.

### **rpcUserHome**

This parameter specifies the home directory of the user. If this value is not specified, the default value is `System.getProperty("user.home")`. If **rpcUser** is specified, you should specify **rpcUserHome**.

### **rpcHost**

This parameter specifies the host on which the RPC mechanism is configured to listen. If this value is not specified, the default value is the value of the **defaultHostName** variable. If your system uses a host other than the **defaultHostName**, set this value accordingly.

### **sudoUser**

If this value is specified, it allows the collective controller to run commands as another, or "sudo", user instead of as the user ID used for the connection. This parameter applies only to servers that have an SSH server installed. This parameter has no default value.

### **sudoPassword**

This parameter specifies the password for the sudo user specified by the **sudoUser** parameter. This parameter applies only to servers that have an SSH server installed. This parameter has no default value.

### **sshPublicKeyPath**

This parameter specifies the path and file name of a user-specified public key file. If this value is not specified, the default is `${server.output.dir}/resources/security/ssh/id_rsa.pub`. If the specified file (or default file) does not exist, a new public key file will be generated.

### **sshPrivateKeyPath**

This parameter specifies the path and file name of a user-specified private key file. If this value is not specified, the default is `${server.output.dir}/resources/security/ssh/id_rsa`. If the specified file (or default file) does not exist, a new private key file will be generated.

### **sshPrivateKeyPassword**

This parameter specifies the password for the private key. This parameter has no default value.

8.5.5.4

### **useHostCredentials**

This parameter specifies whether collective member server commands inherit RPC credentials from the host. The default is `false`, requiring the user to specify RPC credentials for the controller to remotely start or stop the member. When set to `true`, collective member server commands inherit RPC credentials from the host registration and ignore all other RPC credentials in the `hostAuthInfo` configuration element.

## **Examples**

Scenario 1: Server is on Windows operating system, no SSH is installed

```
<hostAuthInfo rpcUserPassword="myPassword"/>
```

Scenario 2: Server has SSH installed, SSH is running on port 2222

```
<hostAuthInfo rpcPort="2222"/>
```

Scenario 3: Need to run commands as another user

```
<hostAuthInfo sudoUser="anotherUser" sudoPassword="anotherPassword"/>
```

Scenario 4: Server is on a Windows operating system and ssh (e.g. Cygwin) is installed. With the following server configuration, the controller connects the member server with ssh. In this case, the requirement to disable Windows User Account Control (UAC) does not apply. The parameter `<user's home directory>` is the user default home directory, for example: `C:\cygwin\home\bob`

```
<hostAuthInfo rpcUserHome="<user's home directory"> />
```

8.5.5.4

Scenario 5: The collective controller and member are on separate hosts, and not on the same host. To specify that the member inherit RPC credentials from the host, set `useHostCredentials` to `true` in the `server.xml` file of the member. Complete the following steps to configure the member to inherit RPC credentials from the host by specifying `--useHostCredentials` in the `join` command that joins a server as a member to the collective.

1. Create, configure, and start a collective controller named `myController` as shown in step 1 of “Configuring a Liberty collective” on page 1136.
2. Register the host for the member with the collective. The member and the collective controller are on different hosts.

In this scenario, the `registerHost` command uses the collective controller host `hostA.ibm.com` with port number 9443, user `admin`, and password `adminpwd`. The command registers the member host `hostB.ibm.com` with the collective, and sets `rpcUser` to an operating system login user ID for the member host `osUser1`, and `rpcUserPassword` to the operating system login password for the user ID for the member host `osUser1Pwd`. Run the `registerHost` command on the collective controller host.

```
wlp/bin/collective registerHost hostB.ibm.com --host=hostA.ibm.com --port=9443 --user=admin --password=adminpwd --rpcUser=osUser1
```

Enter `y` (yes) when prompted to accept the certificate chain. After registration, the Host `hostB.ibm.com` successfully registered. message displays. The collective controller host now has the operating system user ID and password of the member host.

3. On the member host, create a server named `myMember` to use as a collective member.

```
wlp/bin/server create myMember
```

4. Add the `myMember` server to the collective controller, specifying to use host credentials. In the `join` command, which is run on the member host, specify `--useHostCredentials` so that the member inherits RPC credentials from the host registration.

```
wlp/bin/collective join myMember --host=hostA.ibm.com --port=9443 --user=admin --password=adminpwd --keystorePassword=memberKSPas
```

5. Update the member `server.xml` file as shown in step 2 of “Configuring a Liberty collective” on page 1136.

Because you specified `--useHostCredentials` in the `join` command, the configuration generated for the member `server.xml` file sets `useHostCredentials` to `true`:

```
<!-- Remote host authentication configuration -->  
<hostAuthInfo useHostCredentials="true" />
```

With the `--useHostCredentials` option, you do not need to specify the operating system user ID and password in the member `server.xml` file because the member inherits credentials from the host. Later, if the operating system user ID or password of the member server changes, run the `updateHost` command to change the user ID or password. For more information about the `registerHost` and `updateHost` commands, see “Registering host computers with a Liberty collective” on page 1142.

## Starting and stopping a Liberty collective member

8.5.5.0

The collective controller provides a `ServerCommands` MBean that can be used to start or stop a collective member. The MBean `startServer` and `stopServer` methods start and stop a member. You also can run server **start** and **stop** commands from a command line.

## Prerequisites

- The member server must have the `collectiveMember-1.0` feature enabled in its `server.xml` file.
- The member must be joined to the collective. See “Configuring a Liberty collective” on page 1136.

## Set up

To enable the collective controller to stop and start a member server, it might be necessary to add the `<hostAuthInfo>` element to the member's `server.xml` file. By default, each member attempts to use SSH key-based authentication. A pair of RSA keys is generated on server startup under `${server.config.dir}/resources/security/ssh`. The public key is added to the user's `authorized_keys` file automatically. The private key is sent to the controller. If SSH is not available:

- **Windows** For Windows members, you must provide an administrator user ID and password in the `<hostAuthInfo>` element.
- **AIX** **HP-UX** **Linux** **Solaris** **z/OS** For AIX, HP-UX, Linux, Solaris, or z/OS members, use of SSH key-based authentication is recommended. To use a username and password for authentication, specify them in a `<hostAuthInfo>` element in the `server.xml` file.

See “Overriding Liberty server host information” on page 1144 and “Setting up RXA for Liberty collective operations” on page 1491 for details.

## Procedure

- Use the `ServerCommands` MBean `startServer` and `stopServer` methods to start and stop a collective member.

For information on running the `ServerCommands` MBean from the controller, see the API documentation for the `ServerCommands` MBean.

- Run server **start** and **stop** commands from a command line. See “Starting and stopping a server from the command line” on page 1584.

## Registering host computers with a Liberty collective

8.5.5.0

You can register a host computer with a Liberty collective controller, update host information, or unregister a host. Registration enables the collective controller to access applications, command files, and other resources on the host. Registered hosts are members of the collective.

### Before you begin

1. Construct a Liberty collective. See “Configuring a Liberty collective” on page 1136.

#### Distributed operating systems

IBM i

The `collectiveController-1.0` feature and its capabilities are available only in multiple-server products such as WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in single-server products such as WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a multiple-server product installation, you can use its `collectiveController-1.0` feature to work with collective members from single-server products.

2. To enable connections to servers on local and remote hosts, complete the steps for your host operating system in “Setting up RXA for Liberty collective operations” on page 1491. The topic provides information about the Tivoli Remote Execution and Access (RXA) toolkit and enabling Secure Shell

(SSH) protocol. You can use RXA to remotely start and stop servers, including starting and stopping servers on your local computer, and to transfer files to and from registered hosts.

**Note:** Windows In Windows, system environment variables are visible only inside the shell that RXA connects to. Setting PATH in the command window is not sufficient. You must set PATH in the system variable section of the environment variables, or use `-hostJavaHome <PATH TO IBM JAVA>` with the `updateHost` option.

3. If you want to enable a collective controller and its members to use the security TLSv1.2 protocol for the Secure Sockets Layer (SSL) context, see “Setting up Liberty to run in SP800-131a” on page 1848. The `server.xml` files of the controller and members need `ssl id` elements and each host computer needs a `server.env` file with the `JVM_ARGS=-Dhttps.protocols=TLSv1.2` statement in its `${wlp.install.dir}/etc` directory.

## About this task

A host computer is not required to have any WebSphere Application Server products installed. There are no software requirements for a host beyond its operating system. The host can be the same computer on which the product is installed or a different computer.

To register a host with a collective controller, update host information, and unregister a host, use the **registerHost**, **updateHost**, and **unregisterHost** commands. Specify the host computer name in one of the following formats:

- Fully qualified domain name servers (DNS) host name string, such as `xmachine.ibm.com`
- Default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

**Note:** When a Liberty server is joined to a collective, the associated host is automatically registered with the collective controller if it is not already registered.

A host can be registered with the collective under different names. Ensure that the host name specified for **registerHost**, **updateHost**, and **unregisterHost** is consistent with the host name used for the registered collective members. The `defaultHostName` variable in the registered server member's `server.xml` file controls the host name to which the server considers itself to belong.

## Procedure

- Register a host with a collective controller.

To register the current host where both the collective controller host and the remote target host are the same computer, run the **registerHost** command on the collective utility script with no explicit host target. Specify the collective controller's host name, port, and administrative user name and password. For example:

```
wlp/bin/collective registerHost --host=controllerHost --port=controllerHTTPSPort
--user=controllerAdmin --password=controllerAdminPassword
```

This example command generates a unique SSH key pair for authenticating to the SSH server of a specified host computer. If you are registering a remote host for which an SSH key pair is already generated, you can specify the path of the SSH private key file. The following **registerHost** command assumes that the SSH private key is stored on the local controller computer at `/home/user1/.ssh/id_rsa`. The other file in the SSH key pair is the `/home/user1/.ssh/authorized_keys` public key file on the remote target host.

```
wlp/bin/collective registerHost remotehost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
--sshPrivateKey=/home/user1/.ssh/id_rsa
```

If the remote target host does not support SSH or you do not want to use SSH keys, you can specify an operating system login user for `rpcUser` and login password for `rpcUserPassword`. If you include `rpcUser` with `rpcUserPassword`, do not include `sshPrivateKey`. The command to specify operating system login user and password resembles:

```
wlp/bin/collective registerHost remotehost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
--rpcUser=osUserForRemoteHost --rpcUserPassword=osUserPasswordForRemoteHost
```

### 8.5.5.2

To transfer files to and from a host, you must specify host read and write paths. Unless the **registerHost** command specifies the paths, you cannot deploy a Liberty archive to the host. The **hostReadPath** specifies the directories that the collective controller can read. The **hostWritePath** specifies the directories to which the collective controller can write. Paths that are specified by **hostWritePath** are also readable. For example, to upload an archive to /opt/wlp, you must specify **--hostWritePath=/opt**. Specify a parameter multiple times for multiple paths.

```
wlp/bin/collective registerHost myHost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
--rpcUser=osUser --rpcUserPassword=osUserPassword
--hostReadPath=/opt --hostWritePath=/dir1 --hostWritePath=/dir2
```

To use the Deploy tool of the WebSphere Liberty Administrative Center ("Admin Center"), you must set **hostWritePath** to the path to which you want to deploy a server package. To transfer files to multiple directories, include multiple instances of the **hostWritePath** parameter in the command. For example:

```
wlp/bin/collective registerHost myHost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin
--password=controllerAdminPassword --rpcUser=osUser --rpcUserPassword=osUserPassword
--hostWritePath=c:\was\liberty\brokerageAppTest --hostWritePath=c:\wlp_backup
```

### Windows

Before you deploy a server package by using the Deploy tool of Admin Center, complete the steps for your host operating system in "Setting up RXA for Liberty collective operations" on page 1491.

Optionally, specify the path to the Java home directory of the host with the **-hostJavaHome** parameter. For example: **-hostJavaHome=c:\java\jre**

- Update registered host authentication information.

Run the **updateHost** command on the collective utility script to change the authentication information of a registered host. For example, if the user password changes, the following command updates the host password that is used by the collective:

```
wlp/bin/collective updateHost myHost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
--rpcUser=osUser --rpcUserPassword=newOsUserPassword
```

- **8.5.5.2** Update registered host read or write paths.

Run the **updateHost** command on the collective utility script to change the host read and write paths. Paths in this command override the previously set paths for **hostReadPath** and **hostWritePath**, and do not add to the existing paths.

```
wlp/bin/collective updateHost myHost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
--rpcUser=osUser --rpcUserPassword=osUserPassword
--hostReadPath=/optNew --hostWritePath=/opt --hostWritePath=/home/osUser
```

- Unregister a host from a collective controller.

Run the **unregisterHost** command on the collective utility script; for example:

```
wlp/bin/collective unregisterHost myHost.ibm.com --host=controllerHost
--port=controllerHTTPSPort --user=controllerAdmin --password=controllerAdminPassword
```

Unregistering a host removes all the registered servers on that host and any other host-based information from the collective controller.

## What to do next

For information about all parameters of the **registerHost**, **updateHost**, and **unregisterHost** commands, see the API documentation for the `CollectiveRegistration` MBean.

## Configuring Liberty collective replica sets

You can configure collective replica sets. A replica set provides highly available management capabilities for a Liberty administrative domain.

Distributed operating systems

IBM i

### Before you begin

The `collectiveController-1.0` feature and its capabilities are available only in WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a WebSphere Application Server Liberty Network Deployment installation, you can use its `collectiveController-1.0` feature to work with collective members from WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core installations. A collective member can be from any WebSphere Application Server Liberty release.

### About this task

A *replica set* is a set of collective controllers that are configured to work together. Each replica contains all the repository updates that the other replicas within the set have processed. Therefore, there is no need for a member or client to connect with a particular collective controller each time that it interacts with the collective; any of the collective controllers that are configured in the replica set can provide the same data.

For detailed instructions about creating and configuring a collective controller, see “Configuring a Liberty collective” on page 1136.

You can complete the following procedures to configure a collective replica set:

1. Add a replica to an existing replica set.
2. Modify the default configuration of the initial replica set.

See Example: Create and activate a replica set for an example of creating a replica set consisting of three collective controllers on the same host.

### Procedure

1. Add a replica to an existing replica set.

During the life of a replica set, it might become necessary to add one or more replicas to an existing set, to increase capacity for example.

The existing replicas in the replica set do not require any updates to their configuration. You can update them so that their configurations in the `server.xml` files more accurately reflect the replicas that form the replica set, but this update is unnecessary and does not affect their behaviors.

**Note:** It is not necessary to change the `replicaSet` value in the `server.xml` file of an existing replica in the set. No change to the configuration of an existing replica is required. If you do want to update the `replicaSet` values in the configurations of existing replicas in the set so that the configuration values are consistent across all replicas in the set, you must set the `isInitialReplicaSet` value in the configurations of the existing replicas to `false`. After you alter the `replicaSet` value, it describes a changed replica set rather than the initial replica set.

**Note:** When you refer to a replica, you must be consistent and use the same `host:port` value. If a hostname is used, it must always be used. Or, if an IP address is used, it must always be used.

To add a replica, follow these steps:

- a. Ensure that the existing replica set is running and that most of the replicas are available.

- b. Create a server to be the new collective controller.

```
wlp/bin/server create MyNewController
```

- c. Replicate to transform the new server into a collective controller.

```
wlp/bin/collective replicate MyNewController
--host=host_of_running_controller
--port=https_port_of_running_controller
--user=userName_for_running_controller
--password=userPassword_for_running_controller
--keystorePassword=keystore_password_for_new_controller
```

The **replicate** command writes XML output to a console screen. You copy the output into the `server.xml` file.

**8.5.5.2** To write the output of the command to a file, instead of to a console screen, specify the `--createConfigFile=output_file_path` parameter. Then, include the outputted file in the collective configuration by adding an `include` statement to the `server.xml` file:

```
<include location=output_file_path />
```

- d. Configure the new replica's `server.xml` file by using output of the **replicate** command.

Copy the XML output of the **replicate** command into the `server.xml` file. You can modify the replica configuration as follows:

- **Required settings:**

The values must be explicitly set. The XML printed by the **replicate** command contains this configuration and is sufficient for these settings.

**8.5.5.4 hostAuthInfo**

Host authentication information containing properties that a remote client needs to start the server. This setting is only required when the host of the new replica is not enabled for SSH. Typically, Linux hosts are enabled for SSH and Windows hosts are not enabled for SSH. Thus, this setting might only be needed on Windows hosts. Set RPC credentials for the replica in either of two ways:

- Set `rpcUser` to an operating system login user ID for the host on which the replica resides, and set `rpcUserPassword` to the operating system login password for the user ID. For example, if you log into the replica computer with user `test1` and password `test1pwd`, then change the `hostAuthInfo` element to the following:

```
<hostAuthInfo rpcUser="test1" rpcUserPassword="test1pwd" />
```

- If the replica host is registered with the collective controller, set `hostAuthInfo useHostCredentials` to `true` for the replica to inherit RPC credentials from its host.

```
<hostAuthInfo useHostCredentials="true" />
```

See “Overriding Liberty server host information” on page 1144 for information about `hostAuthInfo` settings.

**replicaSet**

Space-delimited list that contains the `host:port` for each of the `replicaHosts` and `replicaPorts` in the replica set, excluding the values for the collective controller now being added to the set

For example,

```
original.host.com:10001 some.other.host.com:10003
```

At least one of the values in this set must already be a replica of the existing replica set.

- **Optional settings:**

These settings default, but can be altered.

**isInitialReplicaSet**

False

**replicaHost**

Hostname for each individual replica

**replicaPort**

Port for each individual replica

This port is not the http or https port of the collective controller, but it is a unique port that is used for communication between the replicas of the replica set.

**repositoryDir**

Directory location that is used to store repository data

Here is an example of what you might add to a new replica `server.xml` file:

```
<collectiveController replicaHost="localhost"
  replicaPort="10012"
  replicaSet="localhost:10010 localhost:10011"
  isInitialReplicaSet="false"/>
```

The XML printed by the **replicate** command requires updating the server's security configuration and specifying the `collectiveRootKeys` keystore password. The server's security configuration should be identical to the original collective controller's configuration, and the `collectiveRootKeys` keystore password should be the password that is used for the original collective controller's `collectiveRootKeys` keystore password. If the replica was created from the controller that is created in "Configuring a Liberty collective" on page 1136, the new controller's configuration should contain the following:

```
<quickStartSecurity userName="adminUser" userPassword="adminPassword" />
<!-- collective root signers keystore -->
<keyStore id="collectiveRootKeys" password="yourPassword"
  location="{server.config.dir}/resources/collective/rootKeys.jks" />
```

- e. Start the new replica by starting the new collective controller.
- f. Confirm that the original collective controller successfully connected to the new replica. Look for message CWWKX6009I in the `messages.log` file of the original collective controller and the replica.

**Tip:** For scripts that run the **replicate** and **addReplica** commands, add a 10-second wait after the **replicate** command runs to ensure the original collective controller and replica connect before running the **addReplica** command.

- g. Invoke the `addReplica` operation on the collective utility to activate the new replica. The argument to the `addReplica` set must be the replica endpoint (in the form "replicaHost:replicaPort") of the replica to add.

```
wlp/bin/collective addReplica localhost:10012
  --host=host_of_running_controller
  --port=port_of_running_controller
  --user=user_for_running_controller
  --password=user_password
```

2. Optional: If necessary, you can modify the default configuration of the initial replica set. This step is recommended but not required.

The configuration of the initial replica set occurs when the initial collective controller is created. If it is necessary to modify the default replica configuration, the following properties can be changed in the `server.xml` file:

**Optional settings:** These values default, but can be altered.

**replicaHost**

Hostname for each individual replica

**replicaPort**

Port for each individual replica

This port is not the http or https port of the collective controller, but it is a unique port that is used for communication between the replicas of the replica set.

**repositoryDir**

Directory location that is used to store the repository data

## Example: Creating and activating a replica set

This example describes how to create a replica set and then activate it. A replica set must have at least three replicas, preferably on different hosts, for high availability. This example has the replicas on the same host, which requires that you assign unique port numbers for the replicas. When replicas are on different hosts, the replicas can use the same port numbers.

### 1. Create a replica set.

To create a replica set, you increase the number of collective controllers and configure them so that they can communicate with each other. Each new collective controller is called a *replica* because the added collective controllers have the same security configuration as the original controller and because all information written to any one controller is automatically replicated to all other active controllers. Once configured, all collective controllers in the replica set can perform the same operations as the original controller.

- a. If you do not have a collective controller, create one. See step 1 of “Configuring a Liberty collective” on page 1136.
- b. Ensure the existing collective controller is running. For an existing controller named `myController`, run the **status** command:

```
wlp/bin/server status myController
```

If the collective controller is not running, then start it using the **start** or **run** command:

```
wlp/bin/server start myController
```

- c. Create a server to be the new collective controller.

```
wlp/bin/server create myController2
```

- d. Replicate the existing collective controller configuration into the new collective controller. The new collective controller is called a *replica*.

Run a **replicate** command that uses the administrative security domain configuration of the existing collective controller and sets a new keystore password for the replica. Look at the `server.xml` file of the existing collective controller to find the values for the `--host`, `--port`, `--user`, and `--password` parameters. For `--keystorePassword`, set a value to use for the keystore, such as `myController2`. For information about these required parameters and about optional parameters, run `collective help replicate` at a command line.

```
wlp/bin/collective replicate myController2 --host=host_of_existing_controller --port=https_port_of_existing_controller --user=userName
```

If prompted to accept the certificate chain, enter `y` (yes).

The **replicate** command writes XML output to a console screen. You copy the output into the `server.xml` file.

**8.5.5.2** To write the output of the command to a file, instead of to a console screen, specify the `--createConfigFile=output_file_path` parameter. Then, include the outputted file in the collective configuration by adding an `include` statement to the `server.xml` file:

```
<include location=output_file_path />
```

- e. Add the XML output of the **replicate** command into the `server.xml` file of the replica and edit the parameter values as needed.
  - Ensure that the `httpEndpoint` element sets `replica httpPort` and `httpsPort` values that are unique port numbers on the host. For example, suppose the original controller named `myController` and the replica are both on the same localhost and `myController` has the following the `httpEndpoint` element:

```
<httpEndpoint id="defaultHttpEndpoint"
  host="*"
  httpPort="9080"
  httpsPort="9443" />
```

Change the values for `myController2` to:

```
<httpEndpoint id="defaultHttpEndpoint"
  host="*"
  httpPort="9085"
  httpsPort="9448" />
```

- **8.5.5.4** Set RPC credentials for hostAuthInfo. You can set RPC credentials for the replica in either of two ways:

- Set hostAuthInfo RPC user and password values. Set rpcUser to an operating system login user ID for the host on which the replica resides, and set rpcUserPassword to the operating system login password for the user ID. For example, if you log into the replica computer with user test1 and password test1pwd, then change the hostAuthInfo element to the following:

```
<hostAuthInfo rpcUser="test1" rpcUserPassword="test1pwd" />
```

- If the replica host is registered with the collective controller, set hostAuthInfo useHostCredentials to true for the replica to inherit RPC credentials from its host.

```
<hostAuthInfo useHostCredentials="true" />
```

See “Overriding Liberty server host information” on page 1144 for information about hostAuthInfo settings.

- Ensure that replicaPort sets a port number for the replica that is unique among the replica set and that replicaSet sets host:port values that identify the replica set. For example, if the original controller named myController and the replica are both on the same localhost, change the values for myController2 from null:

```
<collectiveController replicaPort="null"
  replicaSet="localhost:null"
  isInitialReplicaSet="false" />
```

to 10011 for the replica port and 10010 for the replica set port:

```
<collectiveController replicaPort="10011"
  replicaSet="localhost:10010"
  isInitialReplicaSet="false" />
```

- Ensure the security configuration sets the same values as those used by the original controller. For example, both myController and the myController2 replica use:

```
<quickStartSecurity userName="adminUser" userPassword="adminPassword" />
```

- Ensure the collective root signers keystore element sets the same password as that used by the original controller. For example, copy the collectiveRootKeys keystore password from the myController server.xml file and paste it into the myController2 replica server.xml file. This example shows a generated password:

```
<!-- collective root signers keystore -->
<keyStore id="collectiveRootKeys" password="{xor}Lz4sLCgwLTs="
  location="{server.config.dir}/resources/collective/rootKeys.jks"/>
```

- f. Start the new replica by starting the new collective controller.

```
wlp/bin/server start myController2
```

- g. Verify that the original collective controller can communicate with the new replica.

- 1) Open an editor on the original controller messages log, \$WLP\_USER\_DIR/servers/myController/logs/messages.log.

- 2) Look for the following message, which might have different IP addresses in your environment:

```
CWWKX6009I: The collective controller successfully connected to replica 127.0.0.1:10011. Current active replica set is [127.0.0.1:
```

- h. Verify that the new replica can communicate with the original collective controller.

- 1) Open an editor on the replica messages log, \$WLP\_USER\_DIR/servers/myController2/logs/messages.log.

- 2) Look for the following message, which might have different IP addresses in your environment:

```
CWWKX6009I: The collective controller successfully connected to replica 127.0.0.1:10010. Current active replica set is []. The con
```

2. Activate the new replica.

Run an **addReplica** command that uses the administrative security domain configuration of the collective controller and specifies the endpoint of the replica that you want to activate in the form

*replicaHost:replicaPort*. Look at the `server.xml` file of the collective controller to find the values for the `--host`, `--port`, `--user`, and `--password` parameters. Look at the `server.xml` file of the replica to find the values for *replicaHost:replicaPort*. For information about these parameters, run `collective help addReplica` at a command line.

```
wlp/bin/collective addReplica replicaHost:replicaPort --host=host_of_existing_controller --port=port_of_existing_controller --user=u
```

For this example, which has the existing collective controller and the replica on the same host, `localhost`, run:

```
wlp/bin/collective addReplica localhost:10011 --host=localhost --port=9443 --user=adminUser --password=adminPassword
```

If prompted to accept the certificate chain, enter `y` (yes).

- Repeat steps 1 and 2 for additional replicas. For example, add a third replica to the replica set. Name the new replica `myController3` and specify `replicaPort="10012"`. A replica set must have at least three replicas for high availability.

After the third replica is added to the replica set, you can verify that the original collective controller and new replicas synchronized successfully.

- Look for the following messages in the original controller messages log. The messages might have different IP addresses in your environment:

```
CWWKX6015I: A request to change the active collective controller replica set was received and is now processing. The current active r
```

```
CWWKX6016I: The active collective controller replica set changed successfully. The current active replica set is {127.0.0.1:10010,127
```

```
CWWKX6011I: The collective controller is ready, and can accept requests. The leader is 127.0.0.1:10010. Current active replica set is
```

```
CWWKX6014I: This collective controller replica finished synchronizing the data with the other replicas.
```

- Look for the following messages in the messages logs of the added replicas. The messages might have different IP addresses in your environment:

```
CWWKX6016I: The active collective controller replica set changed successfully. The current active replica set is {127.0.0.1:10010,127
```

```
CWWKX6011I: The collective controller is ready, and can accept requests. The leader is 127.0.0.1:10010. Current active replica set is
```

```
CWWKX8112I: The server's host information was successfully published to the collective repository.
```

```
CWWKX8114I: The server's paths were successfully published to the collective repository.
```

```
CWWKX8116I: The server STARTED state was successfully published to the collective repository.
```

## Automatically sharing configurations among replicas

8.5.5.5

You can configure one collective controller `server.xml` include file in a replica set and automatically update the configuration of other replicas in the set. Automatic sharing of configurations means that you do not need to manually update the configurations of other replicas. Automatic sharing of configurations is especially useful for collectives that use auto scaling.

### Before you begin

Create a replica set. See “Configuring Liberty collective replica sets” on page 1148. The topic includes Example: Create and activate a replica set, an example of creating a replica set consisting of three collective controllers on the same host.

### About this task

You can drop the include file for a controller configuration into the `configDropins/defaults` directory of that controller to automatically update the configuration of replicas. Alternatively, you can use `ControllerConfigMBean` operations to list, add, or remove the shared configuration files of a collective controller.

## Procedure

1. Create a `configDropins` directory for the controller with the configuration you want to share among replicas.

If the controller of the replica set does not already have the `configDropins/defaults` directory, create the `$WLP_USER_DIR/servers/server_name/configDropins/defaults` directory for the controller.

**Note:** For information about precedence among files in `configDropins` subdirectories, see “Using the configuration dropins folder to specify server configuration” on page 1593. The topic mentions both the `configDropins/defaults` directory and a `configDropins/overrides` directory. Controller configurations dropped into a `configDropins/overrides` directory are not shared among replicas. To share configurations among replicas, you must use the `configDropins/defaults` directory.

2. Share the controller configuration with other replicas in the replica set.

- Drop the configuration of the replica set controller into its `configDropins/defaults` directory.

For example, copy the `server.xml` include file of the controller to its `configDropins/defaults` directory.

- Use `ControllerConfigMBean` operations to list, add, or remove the shared configuration files of a collective controller.

Configuration files are stored in the `$WLP_USER_DIR/servers/server_name/configDropins/defaults` directory of the controllers and are shared with the `configDropins/defaults` directory of the replicas.

Use Jython scripts or a Java client such as JConsole to perform the following collective controller `ControllerConfigMBean` operations:

### **listSharedConfig**

The **listSharedConfig** operation lists the files in the shared configuration directory of the replica.

### **addSharedConfig**

The **addSharedConfig** operation adds a configuration to a file and stores the file in the `configDropins/defaults` directory of each replica. You must specify two parameters for the operation:

#### **fileName**

The file name of the controller configuration to share. If you specify a file name that exists in the shared configuration directory, the existing file is overwritten. (String)

**config** The content of a valid `server.xml` include file. (String)

For example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<server>
  <logging traceSpecification="com.ibm.ws.collective.repository.internal.SharedConfigManager=all"/>
</server>
```

### **removeSharedConfig**

The **removeSharedConfig** operation removes a file from the `configDropins/defaults` directory of each replica. You must specify a parameter for the operation:

#### **fileName**

The file name of the controller configuration to delete from the shared configuration directory of each replica. (String)

The controller configuration automatically synchronizes with the configuration dropins directories of every other replica in the replica set. When you add a replica to a controller that automatically shares its configuration, the content of the `configDropins/defaults` directory of the controller is replicated to the new replica. Any changes that you make to scaling policy definitions for one controller automatically synchronize with configurations in the configuration dropins directories of the other replicas.

If the controller configuration does not automatically synchronize with the configuration of other replicas, check the controller and replica logs. Also, if you used the `configDropins/defaults` directory to share the controller configuration, ensure that configuration monitoring is not turned off. By

default, configuration monitoring is enabled. If configuration monitoring is disabled, you can use the FileNotificationMBean to inform the controller of configuration changes, and then the changes are shared with the replicas. Configurations stored by ControllerConfigMBean operations are automatically shared among replicas whether configuration monitoring is enabled or not. See “Controlling dynamic updates” on page 1594.

### Example: Use JConsole to share the controller configuration among replicas

This example describes how you might use JConsole to share the server.xml include file in the controller configDropins/defaults directory with all replicas:

1. Connect JConsole to the collective controller process.
  - a. Ensure the collective controller is running.

```
wlp/bin/server status collective_controller_name
```

Replicas do not need to be running. Replicas that are not running synchronize the shared configuration when they start.
  - b. Start JConsole if it is not running. On Windows, run the `Java_installation\bin\jconsole.exe` file.
  - c. Select the process for the collective controller.  
To use the REST Connector with JConsole to access MBeans remotely through an underlying HTTPS connection, see [Creating remote JMX connections in Liberty](#).
2. Run the ControllerConfigMBean **addSharedConfig** operation in JConsole to add the controller server.xml include file to the configDropins/defaults directory of each replica.
  - a. On the JConsole **MBeans** tab, select the ControllerConfigMBean **addSharedConfig** operation.
  - b. For **fileName**, specify the path of the server.xml include file; for example:

```
$WLP_USER_DIR/servers/collective_controller_name/trace.xml
```
  - c. For **config**, specify the configuration to add; for example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<server>
  <logging traceSpecification="com.ibm.ws.collective.repository.internal.SharedConfigManager=all"/>
</server>
```
  - d. Click **addSharedConfig** to run the operation.
3. Confirm that the operation successfully shared the controller configuration among the replicas.

### Changing the port of a replica

8.5.5.7

To change the port of a replica that is in a replica set which has many replicas, you must stop and start replicas in a specific order and not change the port of at least one replica until after you change the ports of the other replicas.

#### Before you begin

Create a replica set. See “Configuring Liberty collective replica sets” on page 1148. The topic includes Example: Create and activate a replica set, an example of creating a replica set consisting of three collective controllers on the same host.

#### About this task

When you added a replica to a replica set, you specified a port number for the replica. For example, the following element in a replica server.xml file specifies a replica port of 10011:

```
<collectiveController replicaPort="10011"
  replicaSet="localhost:10010"
  isInitialReplicaSet="false" />
```

When a replica set contains only one replica, you can simply change the `replicaPort` value. However, when the replica set has many replicas, you must stop a replica before changing its port. Also, one replica in the replica set must remain running and must not have its port changed until after you change the ports of the stopped replicas successfully.

## Procedure

1. Stop the replicas for which you want to change ports. Do not stop at least one replica or change its port.
2. Change the `replicaPort` value in the `server.xml` files of the stopped replicas.
3. Start the stopped replicas.
4. Check the `messages.log` of the replicas, and verify that the changed replicas can communicate.

Look for the `CWWKX6011I` message in the replica messages to see if the replica synchronized correctly:

```
CWWKX6011I: The collective controller is ready, and can accept requests. The leader is replicaHost:replicaPort. Current active re
```

5. If you want to change the port of the replica that remained running, you now can stop the replica, change its port, restart it, and verify that it can communicate with the other replicas.

## Generating collective controller SSL keys

8.5.5.4

You can use the collective utility **genKey** command to generate a keystore in Java keystore (JKS) format. The keystore contains a personal certificate that enables Secure Sockets Layer (SSL) communication with the collective controller.

### Before you begin

Create a collective controller. See “Configuring a Liberty collective” on page 1136.

- | If you want to enable a collective controller and its members to use the security TLSv1.2 protocol for the Secure Sockets Layer (SSL) context, see “Setting up Liberty to run in SP800-131a” on page 1848. The `server.xml` files of the controller and members need `ssl id` elements and each host computer needs a `server.env` file with the `JVM_ARGS=-Dhttps.protocols=TLSv1.2` statement in its `${wlp.install.dir}/etc` directory.

### About this task

Remote JMX connections to a collective controller use SSL and require suitable SSL keys. The collective utility **genKey** command generates a keystore that contains a personal certificate which the collective controller trusts. The generated keystore also includes a public signer certificate so it can function as a trust store.

For a Java virtual machine (JVM), such as a collective member server or a non-Liberty server, to connect to a collective controller, the JVM must have a keystore that contains a key which the collective controller trusts. The **genKey** command generates this keystore. After the JVM has the keystore, the JVM can connect to the collective controller and the collective controller can return its key. This return of the collective controller key to the JVM is called the *SSL handshake*.

- | For the JVM to add the collective controller key to the JVM truststore, the `--autoAcceptCertificates` option must be used. If the `--autoAcceptCertificates` option is not used, the user is prompted to add the key to the truststore.

## Procedure

Run the collective **genKey** command to generate a JKS keystore.

```
wlp/bin/collective genKey [--host=collectiveControllerHost --port=collectiveControllerHTTPSPort --user=collectiveControllerAdminUser
```

For example, for a collective controller on host *machineA* that uses port 1090 and has a collective controller administrative user *Admin1* with password *Admin1pwd*, run the following command to generate a keystore and set its password to *kspwd*:

```
collective genKey --host=machineA --port=1090 --user=Admin1 --password=Admin1pwd --keystorePassword=kspwd --autoAcceptCertificates
```

This example includes the required settings for the **genKey** command:

**--host=*collectiveControllerHost***

The host name of the target collective controller

**--password=*collectiveControllerAdminUserPassword***

The password of the administrative user for the target collective controller. If no password is defined, you are prompted for the password of the administrative user specified by the **--user** setting.

**--port=*collectiveControllerHTTPSPort***

The HTTPS port number of the target collective controller

**--user=*collectiveControllerAdminUserID***

An administrative user of the target collective controller

**--keystorePassword=*generatedKeystorePassword***

The password for the generated keystore. If you specify a password and no value is defined, you are prompted for a password.

The **genKey** command also has optional settings:

**--autoAcceptCertificates**

Automatically trust SSL certificates during this command.

**--certificateSubject=*DN***

The distinguished name (DN) of the generated SSL certificate. The default DN is:

```
CN=localhost,OU=client,O=ibm,C=usCN=localhost,OU=client,O=ibm,C=usCN=localhost,OU=client,O=ibm,C=us
```

**--certificateValidity=*numberOfDays***

The number of days the generated SSL certificate is valid. The default validity period is 1825 days, or 5 years. The minimum validity period is 365 days.

**--keystoreFile=*filePath***

The file to which the keystore is written. The default is the *key.jks* file in the current directory.

**--key=*key***

A key to use for aes encoding. The product hashes the specified key string to produce an encryption key to use to encrypt and decrypt the password. To provide the key to the server, define a variable *wlp.password.encryption.key* whose value is the key. If you do not specify this option, the product supplies a default key.

## Setting administrative metadata for Liberty resources

8.5.5.5

You can use the *admin-metadata.xml* file to set administrative metadata for server, cluster, application, and runtime resources. Administrative metadata enables you to associate information such as tags, owners, contacts, and notes with resources. The metadata can simplify resource management and make it easier to find information about resources in large topologies. For example, server metadata that shows the owner of a server can assist you in more quickly finding the correct person to contact if the server

requires changes. The `admin-metadata.xml` file uses XML format and does not exist by default. You must create the file and place it in a server configuration directory or in the Liberty runtime etc directory. After placing the `admin-metadata.xml` file in a supported directory, you can view the metadata in Admin Center or augment the metadata through application programming interfaces (APIs).

## Procedure

1. Determine whether you want the `admin-metadata.xml` file to set metadata for a particular server or for all servers in the runtime environment.

**server** An `admin-metadata.xml` file in a server configuration directory sets metadata for the server, its cluster, and its applications. The file path is `${wlp.install.dir}/usr/servers/server_name/admin-metadata.xml` or, if the `$WLP_USER_DIR` variable is set in a `server.env` file or command window, `$WLP_USER_DIR/servers/server_name/admin-metadata.xml`.

### runtime

An `admin-metadata.xml` file in the runtime etc directory sets metadata for runtime resources. The file is visible to all servers that use the runtime environment. The file path is `${wlp.install.dir}/etc/admin-metadata.xml`. The etc directory does not exist by default; you must create the etc directory.

2. Configure administrative metadata in the `admin-metadata.xml` file.
  - a. Create a text file named `admin-metadata.xml` in the location determined in step 1. If the file already exists, open an editor on the file.
  - b. In an editor, specify administrative metadata for any of the following resource objects:
    - `<server>` - Set no more than one server metadata.
    - `<cluster>` - Set no more than one cluster metadata.
    - `<application>` - Set any number of application metadata.
    - `<runtime>` - Set no more than one runtime metadata.

**Restriction:** You cannot set host metadata in an `admin-metadata.xml` file. You must manage host metadata using Admin Center or `AdminMetadataManager` MBean APIs or scripts.

For each resource object, specify up to four types of metadata:

- `tag` - Assign zero or more tags to a resource object. You use a tag to search for resources.
- `owner` - Assign no more than one owner to a resource object. An owner is typically a person or entity responsible for the metadata. The owner can provide a key for the metadata.
- `contact` - Assign zero or more contacts to a resource object. A contact is a person or entity who can provide information about the resource object.
- `note` - Assign no more than one note to a resource object. A note is arbitrary text.

For guidance on file contents, see Example: `admin-metadata.xml` in a server configuration directory and Example: `admin-metadata.xml` in the runtime etc directory.

Tags that contain uppercase characters are converted to lowercase before deployment to the collective repository. Thus, `<tag>MyTag</tag>` in an `admin-metadata.xml` file displays as `mytag` in Admin Center.

- c. Save the file changes.

## Results

Server metadata in the server configuration directory is deployed to, or undeployed from, the collective repository when the following events occur:

- The server joins to the collective controller through the collective **join** command
- The controller or member server starts
- A member is removed from the collective controller through the collective **remove** command
- The `admin-metadata.xml` file changes

The product monitors the `admin-metadata.xml` file after the server starts and dynamically updates server metadata in the collective repository to reflect any file changes.

| **Important:** Ensure the server is running when you delete an admin-metadata.xml file. If an  
| admin-metadata.xml file is deleted while the server is running then the product removes the metadata  
| from the repository. If some elements are deleted from the file when the server is stopped, the product  
| removes those elements from the repository when the server starts. However, if the  
| admin-metadata.xml file is deleted while the server is stopped, the metadata will not be removed from  
| the repository when the server starts.

Cluster metadata is deployed to, or undeployed from, the collective repository when the following events occur:

- A cluster member connects with the controller, such as when a cluster member starts
- The admin-metadata.xml file changes for a cluster member
- The last cluster member is removed, such as when the last cluster member stops

Application metadata is deployed to the collective repository when the following events occur:

- An application is installed on a server or cluster
- The admin-metadata.xml file changes for an application

Runtime metadata is deployed to, or undeployed from, the collective repository when the following events occur:

- A server joins the collective controller through the collective **join** command
- The runtime installation directory (`${wlp.install.dir}`) is unregistered, resulting in undeployment
- No dynamic updating through the file monitor or AdminMetadataManager MBean

The product does not monitor the admin-metadata.xml file in the etc directory. You must restart the server to update the runtime metadata in the collective repository.

**Note:** Changes made to metadata in the repository using Admin Center are not removed unless the resource is completely removed from the collective.

## Example admin-metadata.xml files

The following examples show admin-metadata.xml files for server and runtime metadata:

Example: admin-metadata.xml in a server configuration directory

```
<admin-metadata>

  <server owner="John Doe">
    <tag>servertag1</tag>
    <tag>servertag2</tag>
    <tag>servertag3</tag>
    <contact>Mike</contact>
    <contact>Fred</contact>
    <contact>Susan</contact>
    <note>This server is the best server.</note>
  </server>

  <cluster name="cluster1" owner="Tom Wood">
    <tag>clustertag1</tag>
    <tag>clustertag2</tag>
    <tag>clustertag3</tag>
    <contact>Roger</contact>
    <contact>Steve</contact>
    <contact>David</contact>
    <note>This cluster is the best cluster.</note>
  </cluster>

  <application name="app1" owner="Sam Hardison">
    <tag>appltag1</tag>
    <tag>appltag2</tag>
    <tag>appltag3</tag>
  </application>
</admin-metadata>
```

```

    <contact>Jack</contact>
    <contact>Tom</contact>
    <contact>Michael</contact>
    <note>Liberty 8.5.5.x with IBM JDK</note>
</application>

<application name="app2" owner="Michael Dell">
  <tag>app2tag1</tag>
  <tag>app2tag2</tag>
  <tag>app2tag3</tag>
  <contact>Susan</contact>
  <contact>Roger</contact>
  <contact>Fred</contact>
  <note>Liberty 8.5.5.x with IBM JDK</note>
</application>
</admin-metadata>

```

Example: admin-metadata.xml in the runtime etc directory

```

<admin-metadata>
  <runtime owner="Admin Boss">
    <tag>runtimetag1</tag>
    <tag>runtimetag2</tag>
    <tag>runtimetag3</tag>
    <contact>Steven</contact>
    <note>Liberty 8.5.5.x with IBM JDK</note>
  </runtime>
</admin-metadata>

```

## What to do next

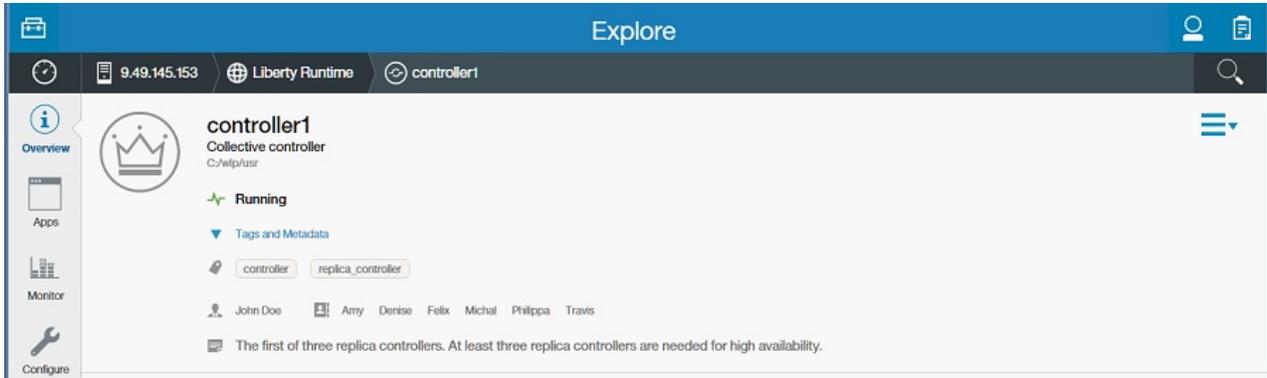
You can view administrative metadata in Admin Center. For example, suppose a collective controller named controller1 has the following admin-metadata.xml file in its server configuration directory, \$WLP\_USER\_DIR/servers/controller1:

```

<admin-metadata>
  <server owner="John Doe">
    <tag>controller</tag>
    <tag>replica_controller</tag>
    <contact>Michal</contact>
    <contact>Felix</contact>
    <contact>Travis</contact>
    <contact>Philippa</contact>
    <contact>Amy</contact>
    <note>The first of three replica controllers. At least three replica controllers are needed for high availability.</note>
  </server>
</admin-metadata>

```

When the controller has <feature>adminCenter-1.0</feature> in its <featureManager> configuration, the Admin Center Explore tool displays the metadata in details about the controller1 server:



**Restriction:** At this time, tags display in the Explore tool only for server, cluster, and application resources. Tags for runtime resources do not display.

For information about viewing administrative metadata in the Explore tool, see “Setting and viewing administrative metadata in Admin Center” on page 1757.

Also, you can use methods in `AdminMetadataManagerMBean` to add, retrieve and set application metadata in the collective repository, as well as remove it from the collective repository.

## Updating a Liberty collective

You can update Liberty collectives by replacing or removing existing collective controllers, members or replica sets or by adding new members or replicas. Before updating a collective, back up its members and replica sets so that you can restore them, if needed, in the future.

### About this task

A Liberty collective can contain members, controllers, and replica sets. See “Liberty: Collective architecture” on page 1450. Over time, you might need to upgrade members or replica sets in the collective or otherwise change the collective configuration.

### Backing up and restoring a Liberty collective

Before changing a collective controller, member or replica set, it is recommended to store a copy of the collective server files so that you can restore the collective, if needed, in the future. You might restore a backed-up copy to fix corrupted files or to downgrade the collective to a previous configuration. When restoring a replica set, it is important to start restored replicas one at a time to synchronize data.

### Procedure

- Back up a collective.

To back up a collective controller, member or replica set, copy the server files that you want to preserve to a safe location. The server files are in the `$WLP_USER_DIR/servers/server_name` directory and its subdirectories. To avoid locking problems when copying the files, stop the server before backing up its files.

- Restore a collective controller or member.

To restore a backed-up collective controller or member server, you can use files in the backed-up directory to configure a new server or, if the Liberty version is the same, copy the backed-up files into the Liberty installation. You do not need to copy the logs and workarea directories into the target installation. Ensure the `server.xml` file of a restored server sets the correct host value and has unique port values in the target installation.

Optionally, start the restored server with the `--clean` parameter to clean cached server information:

```
server start server_name --clean
```

You use the `--clean` option only once; all subsequent server starts do not require it.

- **8.5.5.4** Restore or downgrade a replica set.

1. Stop all replicas in the replica set.

2. Restore the frappe database (`fdb`) directory on one replica from a backup.

Replace the frappe database of the replica that you want to restore with the frappe database of the backed-up replica. The frappe database is the `$WLP_USER_DIR/servers/collective_controller_name/resources/collective/repository/fdb` directory of the replica.

3. Delete the `fdb` directory contents of all other replicas in the replica set.

4. If you want to downgrade to a previous version, replace the Java archive (JAR) files on all replicas with older versions of the JAR files to roll back the replicas to a previous version.

5. Start the replica with the restored `fdb` directory.

6. Look for the `CWWKX6012I` message in the messages for the restored replica.

To see the replica messages, open an editor on the `$WLP_USER_DIR/servers/collective_controller_name/logs/messages.log` file. The message resembles:

```
CWWKX6012I: The collective controller is temporarily unavailable, probably due to a change in the replica set. It should become av
```

7. Start only a minimal majority of the replicas.

Include the restored replica in the number of minimal majority replicas. For example, if a replica set has 5 replicas, a minimal majority is 3 replicas. Because the restored replica is already running, you would start 2 replicas in step 7a.

- a. Start a minimal majority of the replicas.

- b. After these replicas are running, look for the `CWWKX6011I` message in the messages of each replica that you started. The message resembles:

```
CWWKX6011I: The collective controller is ready, and can accept requests. The leader is replicaHost:replicaPort. Current active rep
```

The `CWWKX6011I` message indicates that the replicas synchronized correctly, with the restored `fdb` directory fully replicated in the majority replicas.

Verify that the `[active_replicas]` section in the message lists all the majority replicas that you have started. Also verify that the `[configured_replicas]` section lists all the replicas in the replica set, including replicas that you have not started yet.

8. Start all remaining replicas.

- a. Start the remaining replicas.

- b. After the replicas are running, look for the `CWWKX6011I` message in the messages of each replica.

Verify that the `[active_replicas]` and `[configured_replicas]` sections in the message list all the replicas in the replica set.

The replicas are now running on the restored version.

## Upgrading a Liberty collective

### 8.5.5.4

You can upgrade a collective by replacing existing collective members or replica sets or by adding new members or replicas.

### About this task

A Liberty collective can contain members, controllers, and replica sets. See “Liberty: Collective architecture” on page 1450. Over time, you might need to upgrade replica sets or members in the collective or otherwise change the collective configuration.

### Procedure

- Upgrade a replica set.

1. Choose one replica in the replica set to upgrade. You upgrade replicas one at a time. If the replica is running, stop it.
2. Back up the replica.

You can back up the entire replica server directory, `$WLP_USER_DIR/servers/server_name` directory and its subdirectories. Or, at minimum, back up the frappe database (fdb) directory that holds the replica data, `$WLP_USER_DIR/servers/collective_controller_name/resources/collective/repository/fdb`. See “Backing up and restoring a Liberty collective” on page 1480.

You can use the first replica backup for the remaining replicas.

3. Upgrade the Java archive (JAR) files for the replica. See “Installing Liberty Repository assets” on page 1391.

**Distributed operating systems**

IBM i

Also see “Installing Liberty by extracting a Java archive file” on page 1374.

4. Start the upgraded replica.
5. After the replica is running, look for the CWWKX6011I message in the replica messages to see if the replica synchronized correctly. The message resembles:

CWWKX6011I: The collective controller is ready, and can accept requests. The leader is *replicaHost:replicaPort*. Current active repli

6. After verifying that the replica synchronized, complete steps 1 through 5 for another replica. You can skip step 2 if you use the first replica backup.

Repeat this step 6 until all replicas in the replica set have been upgraded and started one at a time and messages show that the replicas synchronized correctly.

After all replicas are upgraded, the messages.log file for each replica contains message CWWKX6047I, which resembles:

CWWKX6047I: The active collective controller replica set was upgraded successfully. The current active replica version is *version\_num*

- Add a new member to an existing collective.

Use the collective **join** command to add a Liberty server as a member to a collective. See step 2 in “Configuring a Liberty collective” on page 1136.

- Add a new replica to an existing collective.

Use the collective **addReplica** command to add a replica to a collective. See “Configuring Liberty collective replica sets” on page 1148.

## Removing members from a Liberty collective

You can use the collective utility **remove** command to remove a member server from a collective. The **remove** command unregisters the member server from the collective and removes member files that pertain to the collective. The **remove** command does not delete the member server or change the member server.xml file.

### About this task

Administrators of a collective can add a server to the collective using the **join** command and, after the member server is no longer needed, remove the server from the collective using the **remove** command.

The **remove** command can remove a member server that does not exist. For example, the command can remove information about the member from the collective controller in the following situations:

- If the member is deleted accidentally or intentionally
- If deployment fails and the member is partially created or the member configuration contains errors, but the **join** command completed

If the entire wlp/usr user directory on the member host was deleted, you might need to use a client such as JConsole to delete references to the member server from the collective.

## Procedure

1. Stop the member server or remove collective-related elements from the member server configuration.

To stop the member server, run the server **stop** command at a command line:

```
wlp/bin/server stop memberServerName
```

If you want to keep the member server running, remove any of the following elements from the `server.xml` file of the member server:

```
<featureManager>
  <feature>collectiveController-1.0</feature>
  <feature>collectiveMember-1.0</feature>
</featureManager>
<collectiveMember ... />
<hostAuthInfo ... />
```

2. Use a command line to remove a member server.

- a. Run the collective **remove** command at a command line.

```
wlp/bin/collective remove memberServerName --host=collectiveControllerHost --port=collectiveControllerHTTPSPort --user=collectiveControllerAdminUserID
```

For example, for a collective controller on host machineA that uses port 1090 and that has a collective controller administrative user Admin1 with password Admin1pwd and member server member1, run the following command to remove the member server:

```
wlp/bin/collective remove member1 --host=machineA --port=1090 --user=Admin1 --password=Admin1pwd
```

This example includes the required settings for the **remove** command:

**--host=collectiveControllerHost**

The host setting specifies the name of the host on which the collective controller server resides. The defaultHostName variable in the `server.xml` file of the collective controller server sets the host name.

**--port=collectiveControllerHTTPSPort**

The port setting specifies the HTTPS port number of the target collective controller. The httpsPort variable in the `server.xml` file of the collective controller server sets the port number.

**--user=collectiveControllerAdminUserID**

The user setting specifies an administrative user of the target collective controller. A userName variable in the `server.xml` file of the collective controller server sets a user name.

**--password=collectiveControllerAdminUserPassword**

The password settings specifies the password of the administrative user for the target collective controller. A userPassword variable in the `server.xml` file of the collective controller server sets a user password. If no password is defined, you are prompted for the password of the administrative user specified by the **--user** setting.

- b. If prompted to accept a certificate chain, enter y (yes).

The **remove** command deletes the `wlp/usr/servers/member1/resources/collective` directory. The product prints messages resembling the following:

```
Server member1 successfully unregistered.
```

```
Attempting to remove resources for the collective from the server...
The resources for collective membership were successfully removed.
```

Please update the `server.xml` and remove any of the following elements:

```
<featureManager>
  <feature>collectiveController-1.0</feature>
  <feature>collectiveMember-1.0</feature>
</featureManager>
<collectiveMember ... />
<hostAuthInfo ... />
```

- c. If you want to keep the server, complete all instructions in the messages. For example, remove the elements listed in the messages from the `server.xml` file of the removed member server.

If you no longer need the server, delete the server directory. For example, delete `wlp/usr/servers/member1`.

3. If the entire `wlp/usr` user directory was deleted on the member host prior to running the **remove** command, delete any references to the removed member server from the collective using the **delete** operation on a client such as JConsole.
  - a. Connect JConsole to the collective controller process.
    - 1) Ensure the collective controller is running.  
`wlp/bin/server status collective_controller_name`
    - 2) Start JConsole if it is not running. On Windows, run `Java_installation\bin\jconsole.exe`.
    - 3) Select the process for the collective controller.  
To use the REST Connector with JConsole to access MBeans remotely through an underlying HTTPS connection, see *Creating remote JMX connections in Liberty*.
  - b. Run the CollectiveRepository **getDescendantData** operation in JConsole to check for references to the removed member server.
    - 1) On the JConsole **MBeans** tab, select the CollectiveRepository **getDescendantData** operation and specify the name of the node on which the collective resides. The node name resembles `/sys.was.collectives/local/hosts/host_name`; for example, `/sys.was.collectives/local/hosts/machineA`.
    - 2) Look for references to the removed member server in the list of data. If the name of the removed member server is not in the list of data, then the server is no longer a member of the collective. The member was successfully removed from the collective.  
However, if references to the member exist in the data, proceed to the next step. You must run the **delete** operation to remove the member.
  - c. Run the CollectiveRepository **delete** operation in JConsole to delete remaining references to the removed member server from the collective.
    - 1) On the JConsole **MBeans** tab, select the CollectiveRepository **delete** operation.
    - 2) For **nodeName**, specify the fully qualified node name of the member server that you want to delete. The operation deletes the member server node and all nodes under it.  
The node name on a local process where the collective controller is on host machineA and the member path was `C:\wlp\usr\servers\member1` on a Windows computer resembles:  
`/sys.was.collectives/local/hosts/machineA/userdirs/C%3A%2Fwlp%2Fusr/servers/member1`
    - 3) Click **delete**.
  - d. To confirm that the server is no longer a member of the collective, repeat step 2b. Run the CollectiveRepository **getDescendantData** operation in JConsole and check for references to the removed member server.

## Removing a controller from a Liberty collective replica set

During the life of a replica set, it might become necessary to remove one or more replicas from the replica set. You can use the collective utility **removeReplica** command to remove a replica from a replica set. A replica is a collective controller. The **removeReplica** command does not delete the collective controller server.

### About this task

Administrators of a collective can enable a Liberty server to act as a collective controller using the **replicate** and **addReplica** commands and, after the controller is no longer needed, remove the controller from the collective using the **removeReplica** command.

After removal of a replica, the remaining replicas in the replica set do not require any updates to their configuration. However, you might want to update them so that their configurations in the `server.xml` files more accurately reflect the updated replica set.

**Note:** It is not necessary to change the **replicaSet** value in the `server.xml` file of a remaining replica in the set. No change to the configuration of a remaining replica is required. If you do want to update the **replicaSet** values in the configurations of remaining replicas in the set so that the configuration values are consistent across all replicas in the set, you must set the **isInitialReplicaSet** value in the configurations of the remaining replicas to `false`. This is because after you change the **replicaSet** value, it no longer describes the initial replica set; it now describes a changed replica set.

## Procedure

1. Optional: Back up the replica set.
2. Ensure the collective controller is running. For a controller named `myController`, run the **status** command:

```
wlp/bin/server status myController
```

If the collective controller is not running, then start it using the **start** or **run** command:

```
wlp/bin/server start myController
```

3. Remove a collective controller or replica from the replica set.

Run a **removeReplica** command that uses the administrative security domain configuration of the collective controller and specifies the endpoint of the replica that you want to remove in the form `replicaHost:replicaPort`. Look at the `server.xml` file of the collective controller to find the values for the `--host`, `--port`, `--user`, and `--password` parameters. For information about these required parameters and about optional parameters, run `collective help removeReplica` at a command line.

```
wlp/bin/collective removeReplica replicaHost:replicaPort --host=host_of_running_controller --port=https_port_of_running_controller
```

For example, to remove `myController2` from the example replica set in “Configuring Liberty collective replica sets” on page 1148, run the following command:

```
wlp/bin/collective removeReplica localhost:10011 --host=host_of_myController --port=https_port_of_myController --user=user_for_myController
```

## Setting up Liberty server clusters

8.5.5.0

A Liberty can be configured into a server cluster for application high availability and scale.

### Distributed operating systems

IBM i

The `collectiveController-1.0` feature and its capabilities are available only in multiple-server products such as WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in single-server products such as WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a multiple-server product installation, you can use its `collectiveController-1.0` feature to work with collective members from single-server products.

A Liberty server cluster is comprised of two or more Liberty servers configured into a server cluster within a Liberty collective. A Liberty server cluster has a unique name within the collective. The `collectiveController-1.0` feature supports several operations on Liberty server clusters through the `ClusterManager` MBean:

- List clusters
- Start cluster
- Stop cluster
- List cluster members
- Generate cluster plug-in configuration

To be part of a server cluster, a Liberty must be a member of a Liberty collective and also be configured with the `clusterMember` feature.

A collective member can be a member of only one server cluster. All cluster members must be members of the same collective. Multiple server clusters can be configured within the same collective. The following diagram illustrates these relationships.

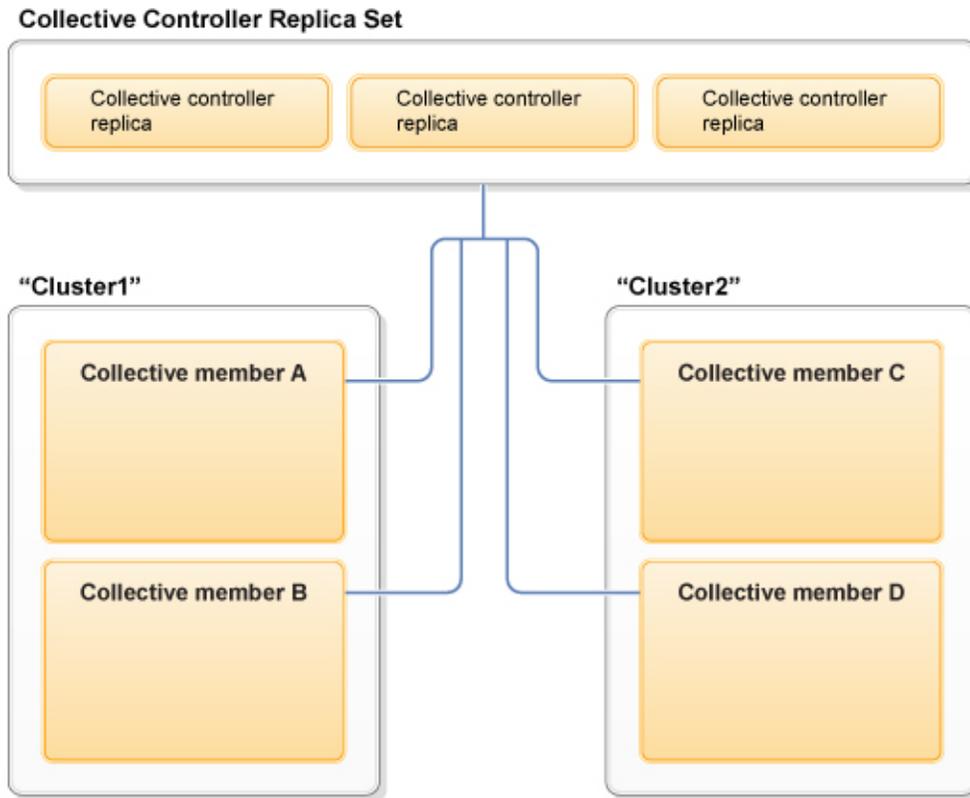


Figure 27. Liberty server clusters

## Configuring a Liberty server cluster

You can configure a collective member to be part of a server cluster by adding the `clusterMember-1.0` feature to the member `server.xml` file. Optionally, you can specify a cluster name to place the member in a particular server cluster. A server cluster has a unique name within a Liberty collective. All Liberty servers that specify the same cluster name within the same collective are members of the same server cluster.

### Before you begin

To be a member of a server cluster, a Liberty server must also be a member of a Liberty collective. If you do not have a Liberty collective and member already, create a collective controller and member server to join the collective. See "Configuring a Liberty collective" on page 1136.

### Procedure

1. Add the `clusterMember-1.0` feature to the feature manager of the member `server.xml` file.
 

```
<featureManager>
  <feature>collectiveMember-1.0</feature>
  <feature>clusterMember-1.0</feature>
</featureManager>
```
2. Optional: To designate that the member belong to a particular server cluster, add a `clusterMember` element that specifies a cluster name.  
For example, place the member in the `myCluster` cluster:

```

<featureManager>
  <feature>collectiveMember-1.0</feature>
  <feature>clusterMember-1.0</feature>
</featureManager>
<clusterMember name="myCluster"/>

```

The default cluster name is `defaultCluster`. If the member `server.xml` does not have a `clusterMember` element that specifies a valid cluster name, then the member is added to `defaultCluster`.

Only specify one cluster name. A single collective can have multiple clusters, but a server can only be part of one cluster at a time.

3. If the collective controller and member server are not running, then start them.

The collective controller and member server must be running for the member to be added to the cluster. For example, use the **start** command to start a collective controller named `myController` and a member named `myMember`:

```
wlp/bin/server start myController
```

```
wlp/bin/server start myMember
```

You can configure a collective member to be a cluster member while the member server is running. The new configuration is updated dynamically and published to the collective controller. If you configure a collective member to be a cluster member while the member server is stopped, the member server will not become a member of a cluster until the server starts.

4. Verify that the member is part of the cluster.

- a. Look for a message that indicates the collective member now belongs to the cluster in the collective controller messages log.

The default path for the log is `${wlp.install.dir}/usr/servers/myController/logs/messages.log` or, if the `$WLP_USER_DIR` variable is set in a `server.env` file or command window, `$WLP_USER_DIR/servers/myController/logs/messages.log`.

```
CWWKX9051I: The myMember server has been added to the myCluster cluster.
```

- b. Look for messages that indicate the collective member is now a cluster member in the member messages log, `$WLP_USER_DIR/servers/myMember/logs/messages.log`.

```
CWWKX7400I: The ClusterMember MBean is available.
           myCluster
```

```
CWWKF0012I: The server installed the following features: [clusterMember-1.0].
```

## What to do next

To enable application security for the cluster, copy the LTPA key file from one of the cluster members to all the other members in the cluster. See “Creating a Liberty cluster with security considerations” on page 1488.

To administer the cluster, you can run collective controller `ClusterManager` MBean operations such as start or stop the server cluster, list clusters and cluster members in the collective, or generate a plug-in configuration file. You can run the operations using Jython scripts or a Java client such as `JConsole`.

**8.5.5.4** Also, you can use WebSphere Liberty Administrative Center (“Admin Center”) to administer the cluster and its servers, applications, and other resources from a web browser. See “Administering Liberty using Admin Center” on page 1741.

**8.5.5.4** After configuring a *static cluster*, which this topic describes, you can route application requests to Liberty servers using IBM HTTP Server (IHS). Static clusters can receive requests through either static or dynamic routing. For information about static routing, see “Generating a Liberty server cluster plug-in configuration” on page 1489. **Distributed operating systems** **z/OS** For information about dynamic routing, see “Setting up dynamic routing for Liberty collectives” on page 1493 and “Generating a plugin-cfg.xml to route to multiple collectives” on page 1499.

**8.5.5.4** To configure an *auto scaling cluster*, which expands and contracts depending on the workload in your environment, see “Setting up auto scaling for Liberty collectives” on page 1503. Auto scaling clusters can receive requests only through dynamic routing.

## Creating a Liberty cluster with security considerations

For secure applications to work in a Liberty clustered environment, all the members in the cluster must have the same LTPA keys.

### About this task

The following information provides details on what must be done for secure applications to work in a Liberty clustered environment when you use IHS or the plug-in.

### Procedure

1. Choose the LTPA key file from one of the cluster members and copy it to all of the other members in the cluster. The default LTPA key file is `${server.ouput.dir}/resources/security/ltpa.keys`.  
Alternatively, you can create a new LTPA key file and store the file at the default location and customize the LTPA key configuration.
2. If the LTPA keys do not dynamically reload after the LTPA key file update, restart the cluster members or enable the dynamic reloading of the LTPA keys. For more information, see “Configuring LTPA in Liberty” on page 1872.

## Starting and stopping a Liberty server cluster

The collective controller provides a `ClusterManager` MBean that can be used to start or stop a Liberty server cluster. The MBean `startCluster` and `stopCluster` methods start and stop all of the members in the cluster serially. To start or stop cluster members individually, you can use `startServer` and `stopServer` methods in the `ServerCommands` MBean or run `server start` and `server stop` commands from a command line.

### Before you begin

- All of the members of the server cluster must have the `clusterMember-1.0` feature enabled in their `server.xml` files.
- All of the members of the server cluster must be configured for collective member starting and stopping. See “Starting and stopping a Liberty collective member” on page 1463 for more information.

### Procedure

- To start and stop all of the servers in the cluster serially, use the `ClusterManager` MBean `startCluster` and `stopCluster` methods. If the size of a cluster is large, the operation can take a long time to complete. The expected execution time is  $O(N)$  where  $N$  is the number of servers in the cluster. The total time for the operation is approximately  $N * (server\_start\_time)$ . If you are starting 100 servers that take 6 seconds to start, for example, the `startCluster` operation will take approximately 600 seconds (10 minutes).
- To start or stop cluster members individually, you can use the `ServerCommands` MBean `startServer` and `stopServer` methods to start and stop a collective member. See “Starting and stopping a Liberty collective member” on page 1463.
- To start or stop cluster members or the collective controller individually, you can run `server start` and `server stop` commands from a command line. See “Starting and stopping a server from the command line” on page 1584.

## Listing Liberty server clusters and cluster members

The collective controller provides a `ClusterManager` MBean that can be used to list Liberty server clusters and cluster members.

## Before you begin

- All of the members of the server cluster must have the `clusterMember-1.0` feature enabled in their `server.xml` files.
- All of the members of the server cluster must be part of a Liberty collective.  
See “Configuring a Liberty collective” on page 1136 for more information.

## Generating a Liberty server cluster plug-in configuration

The collective controller provides a `ClusterManager` MBean that can be used to generate a plug-in configuration file for the HTTP Server for WebSphere Application Server plug-in.

## Before you begin

- All of the members of the server cluster must have the `clusterMember-1.0` feature enabled in their `server.xml` files.
- All of the members of the server cluster must be part of a Liberty collective.
- At least two members of the server cluster must be running when you generate the `plugin-cfg.xml` file.

## Procedure

- Call the `ClusterManager` MBean `generateClusterPluginConfig` operation to create a single, merged `plugin-cfg.xml` file that instructs a web server plug-in to redirect requests to multiple application servers residing on multiple hosts. See “Generating a merged plug-in configuration for Liberty servers” on page 1606.
- For additional information about `plugin-cfg.xml` files, see “Configuring a web server plug-in for Liberty” on page 1604.

## Managing a Liberty server cluster configuration

There are two possible strategies for managing a Liberty server cluster configuration—shared and nonshared.

## About this task

Each Liberty instance comprising a Liberty server cluster has its own configuration documents, such as an `server.xml` file. Although each Liberty instance in a server cluster has unique information in its configuration, such as host name, other information is typically the same across the Liberty instances that comprise the server cluster—deployed applications for example. There are two strategies for managing the configuration for a Liberty server cluster.

## Procedure

- Shared configuration strategy

In this approach, the configuration specification that is common across all cluster members is stored in a common location and included in each cluster member's `server.xml` file using the `<include>` element. See “Using include elements in configuration files” on page 1588 for more information. Changes made to the cluster are made to the shared include.

- Nonshared configuration strategy

In this approach, each cluster member has its own complete `server.xml` file. When you use this strategy, take care when making updates to the cluster members to ensure that each cluster member is updated so that the server cluster remains consistent.

## Liberty cluster troubleshooting

There are common issues that you might encounter with Liberty clusters.

### Problem:

The server is configured to be part of a cluster but the member is not shown to be part of the cluster.

## Solution:

A collective server can be configured to be a cluster member while it is running. The new configuration is dynamically updated and published to the collective controller. If there is a problem publishing to the controller, this will affect the server joining the cluster. If a collective server is configured to be a cluster member while the server is stopped, the server will not be a member of a cluster until the server is started.

## Setting the JAVA\_HOME variable for Liberty collective members

All Liberty collective members must have a Java Runtime Environment (JRE) installed that meets the minimum requirements of the Liberty server. After a JRE is installed on the host computer, you can set the JAVA\_HOME variable so that the Liberty operation can locate the JRE.

### About this task

In order for the collective controller to perform remote operations on Windows members such as starting or stopping a member server, the collective controller must run with an IBM JRE. Third-party JREs do not contain the required security classes. You can get a JRE that supports Liberty products and SSL from Installation Manager offerings or developerWorks:

- Using Installation Manager, select the Liberty product first and then select WebSphere SDK for Liberty. Use Installation Manager to install the Liberty product and software development kit (SDK). The WebSphere SDK for Liberty includes the needed support for Liberty products and SSL and offers a Java client, JConsole.
- Go to <http://www.ibm.com/developerworks/java/jdk/index.html> on the developerWorks website and download an IBM Java development kit (JDK) for your operating system. The developerWorks website does not have a JRE for all operating systems. For example, you have to get the JDK from Eclipse for Windows operating systems.

You can set the JAVA\_HOME variable in operating system settings or at a command line. Setting set the JAVA\_HOME variable enables remote operations to locate the JRE.

### Procedure

- **Windows** To set JAVA\_HOME on a Windows system, perform the following actions.

1. On the Control Panel, do the following:
  - Click **System**.
  - Click **Advanced system settings**.

The System Properties window opens.

2. Click the **Environment Variables** button.
3. Click the *New* button in the system-variables section.
4. Add the JAVA\_HOME variable name and specify a path to the jre directory; for example:  
C:\wlp\_855\IBM\WebSphere\Liberty\java\java\_1.7.1\_64\jre

Some collective controller commands require that the path to the Java installation jre\bin directory be available in the System path, so also add a path to the jre\bin directory.

5. Save the changes. You might need to reboot the computer for the changes to take effect.
6. To verify the changes, at a command line enter set JAVA\_HOME. The command displays the JAVA\_HOME settings; for example:

```
JAVA_HOME=C:\wlp_855\IBM\WebSphere\Liberty\java\java_1.7.1_64\jre
```

**Note:** Rather than change operating system settings, you can set JAVA\_HOME at a command line by entering `set JAVA_HOME=path_to_jre`. A limitation is that the JAVA\_HOME setting only applies to commands entered in the same command window.

- **AIX** **HP-UX** **Linux** **Solaris** If you are running bash shell, you can add the JAVA\_HOME environment variable to the .bashrc file in the user's home directory.
- One option for setting JAVA\_HOME is to create a server.env file in the \${server.config.dir} where server.xml is residing and add JAVA\_HOME there.

For example:

```
JAVA_HOME=/java/jre
```

**Linux** Some collective controller commands require that the path to the Java installation jre/bin directory be available in the .bashrc file, so set a path to jre/bin in the .bashrc file.

## Setting up RXA for Liberty collective operations

Liberty collective controllers use the Tivoli Remote Execution and Access (RXA) toolkit to perform selected operations on collective members. Use RXA to remotely start and stop servers, including starting and stopping servers on your local computer.

### Procedure

- **AIX** **HP-UX** **Linux** **Solaris** **z/OS** **Set up Linux, UNIX or z/OS machines**

Install and enable SSH on your machine. For Linux and UNIX machines, ensure that the configuration is set according to the following instructions. For z/OS machines, consult the following instructions for guidance.

To enable SSH, configure OpenSSH 3.6.1, OpenSSH 4.7 (on AIX), or Oracle SSH 1.1 so that it supports RXA connections. OpenSSH 3.7.1 or later contains security enhancements not available in earlier releases and is recommended.

**Avoid trouble:** OpenSSH Version 4.7.0.5302 for IBM AIX Version 5.3 is not compatible with RXA Version 2.3. If machines are running AIX Version 5.3 with OpenSSH Version 4.7.0.5302 installed, file transfers might not complete. To avoid this problem, revert from OpenSSH Version 4.7.0.5302 to Version 4.7.0.5301.

### Using Secure Shell (SSH) protocol

RXA does not supply SSH code for UNIX operating systems. You must ensure that SSH is installed and enabled on all machines that include collective members.

In all UNIX environments except Solaris, the Bourne shell (sh) is used. On Solaris machines, the Korn shell (ksh) is used instead due to problems encountered with the Bourne shell (sh).

To use password-based authentication for SSH communications, edit the /etc/ssh/sshd\_config file on each machine that includes one or more collective members. Set the PasswordAuthentication property to yes. For example:

```
PasswordAuthentication yes
```

The default value for the PasswordAuthentication property is no.

After you change this setting, stop and restart the SSH daemon by using the following commands:

```
/etc/init.d/sshd stop
/etc/init.d/sshd start
```

**Linux** Some collective controller commands require that the path to the Java installation jre/bin directory to be available in the .bashrc file, so set a path to jre/bin in the .bashrc file.

- **IBM i** **Set up IBM i machines**  
Using SSH public/private key authentication to IBM i machines is not supported.
- **Windows** **Set up Windows machines**
  1. Ensure that your collective controller is running with an IBM JDK.

RXA requires some security classes that are in the IBM JDK, and that are not available in the Oracle or OpenJDK JVMs.

2. Ensure the system environment variables JAVA\_HOME and PATH are set to the Java path (jre directory) on the computer. Some collective controller commands require that the path to the Java installation jre\bin directory is available in the System path, so also add a path to the jre\bin directory.

In Windows, system environment variables are visible only inside the shell that RXA connects to. Setting PATH in the command window is not sufficient. You must set PATH in the system variable section of the environment variables, or use -hostJavaHome <PATH TO IBM JAVA> with the updateHost option.

See "Setting the JAVA\_HOME variable for Liberty collective members" on page 1147.

3. Ensure that the server.xml file of each server to be managed specifies the account user name and password.

Specify the user name and password in a hostAuthInfo statement in the server.xml file:

```
<hostAuthInfo rpcUser="Windows_user_ID" rpcUserPassword="Windows_user_password" />
```

4. Enable connections to member servers on Windows computers.

To enable connections to Windows members, you can use a third-party SSH service such as Cygwin on your Windows member computer or change Windows operating system settings on a member computer that does not have an SSH service installed.

- Use a third-party SSH service such as Cygwin on the Windows member computer.

If the member computer uses an SSH service, the controller connects the member server with SSH. Specify a hostAuthInfo rpcUserHome parameter and the RPC user name and password in the member server.xml file because the third-party SSH service might have a different home directory than the one Windows uses:

```
<hostAuthInfo rpcUser="Windows_user_ID" rpcUserPassword="Windows_user_password" rpcUserHome="user_home_directory"/>
```

For *user\_home\_directory*, specify the user home for the SSH service; for example:

rpcUserHome="C:\cygwin\home\user1". The SSH public and private key pair is generated in the .ssh directory under this user home directory.

- If the Windows member computer does not use a third-party SSH service such as Cygwin, change the Windows operating system settings of the member computer to enable connections.

- Ensure that your user account belongs to the Administrators group.

Many RXA operations require access to resources that standard user accounts cannot access. Thus, the configuration of a collective member must include the name and password of a Windows user who belongs to the Administrators group.

- Ensure File and Printer Sharing for Microsoft Networks is enabled for your network stack.
  - a. Click **Start > Control Panel > Network and Sharing Center > Change advanced sharing settings**.
  - b. Select **Turn on file and printer sharing**.
  - c. Save the changes.

Ensure that file sharing operations (on port 445) are not blocked on machines that include collective controllers or collective members. For more information, see the documentation for your operating system or your firewall software.

- Start the Remote Registry service.

The Remote Registry service must be running on computers that include collective members for the collective controllers to remotely run commands and scripts.

- a. Click **Start > Administrative Tools > Services**.
  - b. Within the list of services, locate the Remote Registry entry and verify that the status is **Started**. If you intend to use RXA regularly, consider setting the Remote Registry **Startup type** property to **Automatic**.
- Disable User Account Control.
    - a. Click **Start > Control Panel > User Accounts > Change User Account Control settings**.

- b. Set the User Account Control level to **Never notify**.
- c. Click **OK**.
- d. Restart the computer for the changes to take effect.

For more information, see *Liberty Collectives Remote Operation Configuration*.

## What to do next

If you modified the `server.xml` of a managed server, manually start the server so that it publishes the new data to the controller.

After you enable RXA, test the host configuration and verify RXA connectivity:

## Setting up dynamic routing for Liberty collectives

8.5.5.4

The Dynamic Routing feature enables routing of HTTP requests to members of Liberty collectives without having to regenerate the WebSphere plug-in configuration file when the environment changes. When servers, cluster members, applications, or virtual hosts are added, removed, started, stopped, or modified; the new information is dynamically delivered to the WebSphere plug-in. Requests will be routed based on up-to-date information. The feature provides the Dynamic Routing service, which dynamically retrieves routing information from the collective repository and delivers this information to the WebSphere plug-in. The feature also provides three new collective command actions. These actions are used together to generate a keystore that is needed for secure communication between the plug-in and the Dynamic Routing service, as well as a plug-in configuration file that enables Intelligent Management in the WebSphere plug-in.

### Before you begin

For the Dynamic Routing function to work, the `dynamicRouting` feature is required in collective controllers only. There is no requirement to upgrade every collective member. Dynamic Routing can be used to route to applications installed in any Liberty server in a collective, including Network Deployment, Core and Base editions.

**Important:** The interim fix for Intelligent Management in the web server plug-in for WebSphere Application Server APAR number PI27023 is necessary to use the Dynamic Routing feature. You must install a web server that is supported by the web server plug-in for WebSphere Application Server, such as the IBM HTTP Server, install an 8.5.5 or higher web server plug-ins for WebSphere Application Server, then install the interim fix before enabling the Dynamic Routing feature.

1. Download and install the latest version of the IBM Installation Manager. For more information on installing IBM Installation Manager, see *Installing Installation Manager and preparing to install the product*.
2. Use Installation Manager to access online product repositories to install the Web Server Plug-in for WebSphere Application Server and the needed interim fix for the Dynamic Routing feature. Open the Installation Manager GUI preferences page by selecting **File > Preferences**. Use the Installation Manager to install the product from the web-based repository that is located at

<http://www.ibm.com/software/repositorymanager/com.ibm.websphere.PLGILAN.v85>

**Note:** You need an IBM ID to access the repository. This repository is only for Distributed platforms.

3. Use the Install wizard to install both the web server plug-ins and the required interim fix.
4. When prompted by the wizard, specify the installation location and proceed with the installation.

 **Watch:** The *Enabling IHS for Liberty Dynamic Routing* video shows how to install IHS, install Web Server Plug-in for WebSphere Application Server, and apply the interim fix for Dynamic Routing. [Transcript]

## About this task

To use Intelligent Management to route HTTP requests to a Liberty Collective the user must enable the **Dynamic Routing** feature on one or more collective controllers in a collective.

### Procedure

1. Enable Dynamic Routing in a controller by adding the following code to the **featureManager** tag in the `server.xml` of the controller.

```
<feature>dynamicRouting-1.0</feature>
```

2. Start all of the controllers that have the Dynamic Routing feature enabled.

3. Run the **dynamicRouting setup** command on one of the controllers to generate the keystore and plug-in configuration files. For example:

```
./dynamicRouting setup --port=9444 --host=controller1.acme.com --user=admin --password=passw0rd --keystorePassword=webAS --pluginIns
```

For more information on Dynamic Routing commands, see “Dynamic Routing Liberty collective command actions” on page 1495.

**Note:** Make sure a specified user name (value of the `--user` argument) is present in a user registry and has an administrative role assigned.

4. Copy the generated `plugin-key.jks` and `plugin-cfg.xml` files to a temporary directory on the web server host.

5. On the web server host, run `gskcmd` (included in the IHS package) to convert the keystore to CMS format and to set personal certificate as the default. CMS format is the supported format of the WebSphere Plug-in. For example:

```
gskcmd -keydb -convert -pw webAS -db /tmp/plugin-key.jks -old_format jks -target /tmp/plugin-key.kdb -new_format cms -stash  
gskcmd -cert -setdefault -pw <<password>> -db /tmp/plugin-key.kdb -label default
```

For z/OS, see “Conversion of the keystore to CMS format on z/OS” on page 1502.

6. Copy the `plugin-key.kdb`, `plugin-key.rdb`, and `plugin-key.sth` files that are created by `gskcmd` from the temporary directory to the directory `<value of the --pluginInstallRootargument>/config/<web server name>/`

7. Copy the `plugin-cfg.xml` to the directory specified in the **WebSpherePluginConfig** directive in the IBM HTTP Server (IHS) `httpd.conf` file. The `plugin-cfg.xml` is generated with the `<IntelligentManagement>` stanza. When Dynamic Routing is enabled in a collective, there is one `<Connector>` stanza for each collective controller.

For example:

```
<IntelligentMangement>  
<Property name="webserverName" value="webServer1"/>  
<ConnectorCluster enabled="true" maxRetries="-1" name="default" retryInterval="60">  
<Property name="uri" value="/ibm/api/dynamicRouting"/>  
<Connector host="controller1.acme.com" port="9444" protocol="https">  
<Property name="keyring" value="/opt/HTTPServer_Plugins/config/webserver1/plugin-key.kdb"/>  
</Connector>  
</ConnectorCluster>  
</IntelligentManagement>
```

8. Start the web server and begin routing to the application installed in the collective.

Optionally, the `<dynamicRouting>` tag can be added to the `server.xml` of the controller to specify `<ConnectorCluster>` properties such as **maxRetries** and **retryInterval**. For example:

```
<dynamicRouting maxRetries="4" retryInterval="20" connectorClusterName="collective1"/>  
<TraceSpecification name="default" specification=":DEBUG"/>  
</dynamicRouting>
```

The generated `plugin-cfg.xml` looks like this:

```
<IntelligentMangement>  
<TraceSpecification name="default" specification=":DEBUG"/>  
<Property name="webserverName" value="webServer1"/>  
<ConnectorCluster enabled="true" maxRetries="4" name="collective1" retryInterval="20">  
<Property name="uri" value="/ibm/api/dynamicRouting"/>  
<Connector host="controller1.acme.com" port="9444" protocol="https">
```

```
<Property name="keyring" value="/opt/HTTPServer_Plugins/config/webServer1/plugin-key.kdb"/>
</Connector>
</ConnectorCluster>
</IntelligentManagement>
```

## Results

With the **Dynamic Routing** feature enabled, Intelligent Management can now dynamically route HTTP requests to Liberty collectives.

## Dynamic Routing Liberty collective command actions

8.5.5.4

The **setup**, **genPluginCfg**, and **genKeystore** dynamicRouting command actions are used to generate the plug-in configuration and keystore files. The **genPluginCfg** dynamicRouting command action is used any time after the initial setup to regenerate the `plugin-cfg.xml` file. For example, when the **Dynamic Routing** feature is enabled on a new controller or a new web server is added. The **genKeystore** dynamicRouting command action is used to generate the keystore file. Each of the dynamicRouting command actions supports online help.

The commands for the **Dynamic Routing** feature are:

- `setup`
- `genPluginCfg`
- `genKeystore`

### setup

The **setup** dynamicRouting command generates a keystore in PKCS12 or JKS format and one or more WebSphere plug-in configuration files. The keystore contains a personal certificate and both the **memberRoot** and **controllerRoot** signer certificates that allow secure communication between the WebSphere plug-in and the Dynamic Routing service. The same keystore is also be used to send HTTPS requests to applications in the Liberty collective members. The plug-in configuration file contains the `<IntelligentManagement>` stanza, which enables Intelligent Management in a WebSphere plug-in. The `<IntelligentManagement>` stanza contains one `<ConnectorCluster>` stanza that represents the collective. The `<ConnectorCluster>` stanza contains one `<Connector>` stanza for each controller where the **Dynamic Routing** feature is enabled.

To get command help, issue `<Controller root>/bin/dynamicRouting help setup`, which displays:

#### Description

The **setup** dynamicRouting command generates a keystore that contains a personal certificate and signer certificates that are required to enable secure communication between the Dynamic Routing service and clients. It also generates WebSphere plug-in configuration file with `<IntelligentManagement>` stanza, which enables Intelligent Management in the WebSphere plug-in.

#### Usage

`dynamicRouting setup [options]`

#### Options

**--host=name**

Required. The host name of the target Collective Controller.

- password[=pwd]**  
Required. The password for the Administrator user for the target Collective Controller. If no value is defined, you are prompted.
- port=num**  
Required. The HTTPS port number of the target Collective Controller.
- user=name**  
Required. An Administrator user for the target Collective Controller.
- pluginInstallRoot=path**  
Required. Fully qualified path of the WebSphere plug-in root directory on the web server host.
- webServerNames=webServerName[,webServerName1]**  
Required. Comma separated names of the web servers for which WebSphere plug-in configuration files need to be generated.
- keystorePassword[=pwd]**  
Required. The password for the generated keystore. If specified and no value is defined, you are prompted.
- keystoreType=type**  
Optional. The type of the generated keystore. Default type is *JKS*. Valid values are *JKS* and *PKCS12*.
- certificateSubject=DN**  
The DN for the generated SSL certificate. The default value, if unspecified is `CN=<value of --user argument>,OU=client,O=ibm,C=us`.

**Note:** When you use an LDAP user registry, you must specify the fully qualified DN of the administrator by using **--certificateSubject** as the default form is probably not valid for your LDAP.

SSL certificates can be automatically trusted by setting the JVM property `com.ibm.websphere.collective.utility.autoAcceptCertificates` to **true**.

**Note:** The keystore that is generated by the **setup** and **genKeystore** commands is in *JKS* or *PKCS12* format. It needs to be copied to a directory on the web server machine and converted to a CMS formatted store by running **gskcmd**. The CMS formatted store file (*.kdb*) must be moved to the directory `<value of the --pluginInstallRoot argument>/config/<web server name>`. The *.rdb* and *.sth* files must also be moved to the same directory.

Following is the output of the command when run with all required arguments:

```
./dynamicRouting setup --port=9444 --host=controller1.acme.com --user=admin --password=password
--keystorePassword=keypass --pluginInstallRoot=/opt/HTTPServer_Plugins
--webServerNames=webServer1,webServer2
```

```
Generating WebSphere plug-in configuration files for web servers webServer1, webServer2
```

```
Auto-accepting the certificate chain for target server.
Certificate subject DN: CN=admin, OU=controller1, O=ibm, C=us
```

```
Successfully completed MBean request to the controller.
Successfully generated WebSphere plug-in configuration files plugin-cfg-webServer1.xml, plugin-cfg-webServer2.xml
Generating keystore for web servers webServer1, webServer2
Successfully completed MBean request to the controller.
Successfully generated keystore plugin-key.jks.
```

```
Generated WebSphere plug-in configuration files plugin-cfg-webServer1.xml, plugin-cfg-webServer2.xml for web servers webServer1, webServer2
Also generated keystore file plugin-key.p12 that enables secure communication between the Dynamic Routing service and client
```

Copy the WebSphere plug-in configuration file to the directory specified in the `WebSpherePluginConfig` directive in the IBM HTTP Server `httpd.conf` file.

Copy keystore file plugin-key.jks to a directory on the web server host, and run "gskcmd" to convert the keystore to CMS format and to set personal certificate as the default.  
For example:

```
gskcmd -keydb -convert -pw <<password>> -db /tmp/plugin-key.jks -old_format jks -target /tmp/plugin-key.kdb -new_format  
gskcmd -cert -setdefault -pw <<password>> -db /tmp/plugin-key.kdb -label default
```

Copy resulting /tmp/plugin-key.kdb, .sth, .rdb files to the directory /opt/HTTPServer\_Plugins/config/webServer1/

## genPluginCfg

This action generates the plug-in configuration files. Each plug-in configuration file contains the <IntelligentManagement> stanza, which enables the Intelligent Management features of the plug-in. The <IntelligentManagement> stanza contains one <ConnectorCluster> stanza that represents the collective. The <ConnectorCluster> stanza contains one <Connector> stanza for each controller where **Dynamic Routing** feature is enabled. Comma-separated web server names are specified to the --webServerNames argument. For example, if --webServerNames=webServer1,webServer2 is specified, plugin-cfg-webServer1.xml and plugin-cfg-webServer2.xml files are generated.

To get online help, issue <Controller root>/bin/dynamicRouting help genPluginCfg, which displays:

### Description

Generates a WebSphere plug-in configuration file with a <IntelligentManagement> stanza that enables Intelligent Management in the WebSphere plug-in.

### Usage

dynamicRouting **genPluginCfg** [options]

### Options

**--host=name**

Required. The host name of the target Collective Controller.

**--password[=pwd]**

Required. The password for the Administrator user for the target Collective Controller. If no value is defined, you are prompted.

**--port=num**

Required. The HTTPS port number of the target Collective Controller.

**--user=name**

Required. An Administrator user for the target Collective Controller.

**--pluginInstallRoot=path**

Required. Fully qualified path of the WebSphere plug-in root directory on the web server host.

**--webServerNames=webServerName[,webServerName1]**

Required. Comma separated names of the web servers for which WebSphere plug-in configuration files need to be generated.

SSL certificates are automatically trusted by setting the JVM property com.ibm.websphere.collective.utility.autoAcceptCertificates to **true**.

Following is the output of the command when run with all required arguments:

```
./dynamicRouting setup --port=9444 --host=controller1.acme.com --user=admin --password=password
--keystorePassword=keypass --pluginInstallRoot=/opt/HTTPServer_Plugins
--webServerNames=webServer1,webServer2
```

This action generates the plug-in configuration files.

Generating WebSphere plug-in configuration file for web server webServer1

Auto-accepting the certificate chain for target server.  
Certificate subject DN: CN=admin, OU=controller1, O=ibm, C=us

Successfully completed MBean request to the controller.  
File /home/user1/Liberty/wlp/bin/plugin-cfg.xml exists.  
Saving to /home/user1/Liberty/wlp/bin/plugin-cfg.xml.old.  
Successfully generated WebSphere plug-in configuration file plugin-cfg.xml

Generated WebSphere plug-in configuration file plugin-cfg.xml for web server webServer1.  
Copy the WebSphere plug-in configuration file to the directory specified in the WebSpherePluginConfig directive in the IBM

## genKeystore

This action generates a keystore in PKCS12 or JKS format. Use the **--keystoreType** action to specify the keystore format. Generation of the PKCS12 keystore is only supported when you use IBM Java. The keystore contains a personal certificate and both the **memberRoot** and **controllerRoot** signer certificates that allow secure communication between the WebSphere plug-in and the Dynamic Routing service. The same keystore is also be used to send HTTPS requests to applications in the Liberty collective members.

To get online help, issue **<Controller root>/bin/dynamicRouting help genKeystore**, which displays:

### Description

Generates a keystore that contains a personal certificate and signer certificates that are required to enable secure communication between the Dynamic Routing service and clients.

### Usage

dynamicRouting **genKeystore** [options]

### Options

**--host=name**

Required. The host name of the target Collective Controller.

**--password[=pwd]**

Required. The password for the Administrator user for the target Collective Controller. If no value is defined, you are prompted.

**--port=num**

Required. The HTTPS port number of the target Collective Controller.

**--user=name**

Required. Specifies an Administrator user for the target Collective Controller.

**--keystorePassword[=pwd]**

Required. The password for the generated keystore. If specified and no value is defined, you are prompted.

**--keystoreType=type**

Optional. The type of the generated keystore. Default type is *JKS*. Valid values are *JKS* and *PKCS12*.

### **--certificateSubject=DN**

The DN for the generated SSL certificate. The default value, if unspecified is CN=<value of --user argument>,OU=client,O=ibm,C=us.

**Note:** When you use an LDAP user registry, you must specify the fully qualified DN of the administrator by using **--certificateSubject** as the default form is probably not valid for your LDAP.

SSL certificates are automatically trusted by setting the JVM property `com.ibm.websphere.collective.utility.autoAcceptCertificates` to **true**.

Following is the output of the command when run with all required arguments:

```
./dynamicRouting genKeystore --port=9444 --host=contoller1.acme.com --user=admin  
--password=password --keystorePassword
```

```
Enter password --keystorePassword:  
Re-enter password --keystorePassword:
```

```
Auto-accepting the certificate chain for target server.  
Certificate subject DN: CN=admin, OU=mycontroller, O=ibm, C=us
```

```
Generating keystore...  
Successfully completed MBean request to the controller.  
Successfully generated keystore plugin-key.jks.
```

Generated keystore file `plugin-key.jks` that enables secure communication between the Dynamic Routing service and clients. Copy keystore file `plugin-key.jks` to a directory on the web server host, and run "gskcmd" to convert the keystore to CMS. For example:

```
gskcmd -keydb -convert -pw <<password>> -db /tmp/plugin-key.jks -old_format jks -target /tmp/plugin-key.kdb -new_format CMS  
gskcmd -cert -setdefault -pw <<password>> -db /tmp/plugin-key.kdb -label default
```

Copy resulting `/tmp/plugin-key.kdb`, `.sth`, `.rdb` files to the keyring directory specified in the WebSphere plug-in configuration.

## **Generating a plugin-cfg.xml to route to multiple collectives**

8.5.5.4

Generate a `plugin-cfg.xml` that enables Intelligent Management in the WebSphere plug-in to route to multiple collectives.

### **Procedure**

1. For each collective that you want Intelligent Management in the WebSphere plug-in to route requests to, do the following:
  - a. Select a collective controller
  - b. Edit the `server.xml` of the collective controller and add the `dynamicRouting` tag. Specify a unique name for the `connectorClusterName` property. For example: `<dynamicRouting connectorClusterName="collective1" />`
  - c. On the selected collective controller machine, use the following collective **dynamicRouting setup** command to generate the `plugin-cfg.xml` and `plugin-key.p12` files.

```
<Liberty server root>/bin/dynamicRouting setup --port=<controllerport> --host=<controller host> --user=<administrator id> --password=<administrator password>  
--keystorePassword=<keystore password> --pluginInstallRoot=<root directory of the  
WebSphere plugin on the WebServer host> --webServerNames=<web server name>  
--keystoreType=pkcs12
```
2. Merge `<ConnectorCluster>` tags from the generated `plugin-cfg.xml` files.
  - a. Copy the `<ConnectorCluster>` elements from all `plugin-cfg.xml` files into one `plugin-cfg.xml` file.

For example, if you have two collectives, copy `<ConnectorCluster>` stanza from `plugin-cfg.xml` of the "collective2" into the `plugin-cfg.xml` of the "collective1".

The merged `plugin-cfg.xml` file appears similar to the following example:

```
<?xml version="1.0" encoding="UTF-8"?><!--HTTP server plug-in config file for defaultServer generated on 2014.05.13
<Config ASDisableNagle="false" AcceptAllContent="false" AppServerPortPreference="HostHeader" ChunkedResponse="false"
  <Property Name="ESIEnable" Value="true"/>
  <Property Name="ESIMaxCacheSize" Value="1024"/>
  <Property Name="ESIInvalidationMonitor" Value="false"/>
  <Property Name="ESIEnableToPassCookies" Value="false"/>
  <Property Name="PluginInstallRoot" Value="/opt/IBM/HTTPServer_Plugins/">
  <!-- Configuration generated using httpEndpointRef=defaultHttpEndpoint-->

  <Property Name="Keyfile" Value="/opt/IBM/HTTPServer_Plugins/config/webserver1/plugin-key-collective1.kdb"/>
  <Property Name="Stashfile" Value="/opt/IBM/HTTPServer_Plugins/config/webserver1/plugin-key-collective1.sth"/>

  <IntelligentManagement>
  <TraceSpecification name="default" specification=":DEBUG"/>
  <Property name="webserverName" value="webserver1"/>

  <ConnectorCluster enabled="true" maxRetries="10" name="collective1" retryInterval="30">
  <Property name="uri" value="/ibm/api/dynamicRouting"/>
  <Connector host="controller1.acme.com" port="9443" protocol="https">
  <Property name="keyring" value="/opt/IBM/HTTPServer_Plugins/config/webserver1/plugin-key-collective1.kdb"/>
  </Connector>
  </ConnectorCluster>

  <ConnectorCluster enabled="true" maxRetries="10" name="collective2" retryInterval="30">
  <Property name="uri" value="/ibm/api/dynamicRouting"/>
  <Connector host="controller2.acme.com" port="9443" protocol="https">
  <Property name="keyring" value="/opt/IBM/HTTPServer_Plugins/config/webserver1/plugin-key-collective2.kdb"/>
  </Connector>
  </ConnectorCluster>

  </IntelligentManagement>
</Config>
```

3. For each collective, convert the pkcs12 formatted keystore to a CMS format.

- a. Copy generated `plugin-key-<connectorClusterName>.p12` file to `/tmp` directory on the IHS host.
- b. Run `gskcmd` to convert it to a CMS formatted store as instructed in the **dynamicRouting setup** command output.

```
./gskcmd -keydb -convert -pw <<password>> -db /tmp/plugin-key-collective1.p12 -old_format p12 -target /tmp/plugin-key-
```

- c. Copy resulting `.kdb`, `.sth` and `.rdb` stores to the `<plugininstallRoot>/config/<webServerName>` directory.

4. Extract all memberroot certificates from each collective `kdb` store and import it into a new keystore, which is used for front-end user requests over SSL.

For example, run the following command to extract the memberroot certificate:

```
./gskcmd -cert -extract -db /tmp/plugin-key-collective1.kdb -label memberroot -pw <<password>> -target /tmp/memberroot.
```

Create a new CMS formatted store that is called `plugin-key.kdb`, and import the memberroot certificates into it.

```
./gskcmd -cert -add -db /tmp/plugin-key.kdb -pw <<password>> -file /tmp/memberroot.cer -label memberroot
```

Copy the resulting plugin-key `.kdb`, `.sth` and `.rdb` files to the `<plugininstallRoot>/config/<webServerName>` directory.

5. Modify the merged `plugin-cfg.xml` to change the `keyfile` and `Stashfile` properties to use the `plugin-key.kdb` and `plugin-key.sth`. The modified `plugin-cfg.xml` appears similar to the following example:

```
<?xml version="1.0" encoding="UTF-8"?><!--HTTP server plug-in config file for defaultServer generated on 2014.05.13 at 1
  <Config ASDisableNagle="false" AcceptAllContent="false" AppServerPortPreference="HostHeader" ChunkedResponse="false"
  <Log LogLevel="Error" Name="/opt/IBM/HTTPServer_Plugins/logs/webserver1/http_plugin.log"/>
  <Property Name="ESIEnable" Value="true"/>
```

```

<Property Name="ESIMaxCacheSize" Value="1024"/>
<Property Name="ESIInvalidationMonitor" Value="false"/>
<Property Name="ESIEnableToPassCookies" Value="false"/>
<Property Name="PluginInstallRoot" Value="/opt/IBM/HTTPServer_Plugins/" />
<!-- Configuration generated using httpEndpointRef=defaultHttpEndpoint-->

<Property Name="Keyfile" Value="/opt/IBM/HTTPServer_Plugins/config/webserver1/plugin-key.kdb"/>
<Property Name="Stashfile" Value="/opt/IBM/HTTPServer_Plugins/config/webserver1/plugin-key.sth"/>

<IntelligentManagement>
  <TraceSpecification name="default" specification=":DEBUG"/>
  <Property name="webserverName" value="webserver1"/>

  <ConnectorCluster enabled="true" maxRetries="10" name="collective1" retryInterval="30">
    <Property name="uri" value="/ibm/api/dynamicRouting"/>
    <Connector host="controller1.acme.com" port="9443" protocol="https">
      <Property name="keyring" value="/opt/IBM/HTTPServer_Plugins/config/webserver1/plugin-key-collective1.kdb"/>
    </Connector>
  </ConnectorCluster>

  <ConnectorCluster enabled="true" maxRetries="10" name="collective2" retryInterval="30">
    <Property name="uri" value="/ibm/api/dynamicRouting"/>
    <Connector host="controller2.acme.com" port="9443" protocol="https">
      <Property name="keyring" value="/opt/IBM/HTTPServer_Plugins/config/webserver1/plugin-key-collective2.kdb"/>
    </Connector>
  </ConnectorCluster>

</IntelligentManagement>
</Config>

```

## Enabling Intelligent Management in the WebSphere plug-in trace

8.5.5.4

Intelligent Management in the WebSphere plug-in trace is enabled by using the **<traceSpecification>** tag.

### About this task

Use the **<traceSpecification>** tag to enable both control and request-based tracing. To enable this tracing, see, *Configuring trace on the web server plug-in*.

For more information on the properties of the **<traceSpecification>** tag, see “Dynamic Routing” on page 872.

### Procedure

1. To set the **:DEBUG** control trace for *webserver1* and *webserver2*, add the following code to the *server.xml* of the controller.

```

<dynamicRouting>
  <traceSpecification name="default" specification=":DEBUG" webservers="webserver1, webserver2" />
</dynamicRouting>

```

This change is communicated to the web server if it is already connected to the Dynamic Routing service.

**Note:** Set the **name** parameter to **default** to use the control trace specification. See *Configuring trace on the web server plug-in* for more information.

Configure different control trace specifications for different web servers. For example:

```

<dynamicRouting>
  <traceSpecification name="default" specification=":DEBUG" webservers="webserver1" />
  <traceSpecification name="default" specification="request.http:DEBUG" webservers="webserver2" />
</dynamicRouting>

```

2. To configure request-based trace specifications for *webserver1*, add the following code to the *server.xml* of the controller.

```
<dynamicRouting>
  <traceSpecification name="custom1" specification="request.http:DEBUG" condition="uri = '/foo'" webservers="webserver1"
</dynamicRouting>
```

**Note:** The **condition** property is required for request-based trace specifications. The **condition** property specifies an expression that is evaluated by Intelligent Management in the plug-in for each request. The specified trace specification is set for the requests that match the expression. For information regarding the format of the condition parameter, see *Configuring trace on the web server plug-in*.

Request-based trace specifications are evaluated in the order they are specified. If two trace specifications with same name are specified, the one that comes later takes precedence. In the following example, *control.process:DEBUG* is used for the control specification for *webserver1*:

```
<dynamicRouting>
  <traceSpecification name="default" specification=":DEBUG" webservers="webserver1" />
  <traceSpecification name="default" specification="control.process:DEBUG" webservers="webserver1" />
</dynamicRouting>
```

Use "\*" to set the trace specification for all the web servers that are connected to the Dynamic Routing service. If you have a specification value that contains actual webserver names, the webserver specification replaces the "\*" specification, regardless of order, because of specificity. The order replacement occurs when both specifications are equally targeted for "\*" or for the same webservers.

```
<dynamicRouting>
  <traceSpecification name="default" specification=":DEBUG" webservers="*" />
  <traceSpecification name="custom1" specification="http.request.rules:DEBUG" condition="uri = '/foo'" webservers="webserver1" />
  <traceSpecification name="custom2" specification="http.response:DEBUG" condition="uri = '/foo'" webservers="webserver1" />
  <traceSpecification name="custom3" specification="http.request.select:DEBUG" condition="virtualhost = 'ibm.com'" webservers="webserver1" />
</dynamicRouting>
```

## Conversion of the keystore to CMS format on z/OS

You can set up dynamic routing for Liberty collectives on a z/OS system. An element of that task is to convert the keystore to a CMS format.

The sample script that is provided here is a suggestion of how to set up the CMS provider for the **ikeycmd**. However, your environment might be different and you must ensure that you locate the CMS provider and specify the correct provider offset.

Both the **gskcmd** commands in step 5 of *Setting up dynamic routing for Liberty collectives* must be run for z/OS by using **ikeycmd** in place of **gskcmd**. The **ikeycmd** commands must include the additional `-Djava.security.properties` as indicated in the sample script to append the CMS provider with an appropriate provider offset. The `-Djava.security.properties` parameter must precede the other parameters that are specified in step 5 of *Setting up dynamic routing for Liberty collectives* for each command.

```
#!/bin/sh

# z/os ikeycmd wrapper that adds CMS v3 support.
# Author:

if [ -n "$JAVA_HOME" ]; then
  echo "Using JAVA_HOME=$JAVA_HOME"
else
  JAVA_HOME=/usr/lpp/java/java800/J8.0_64/
fi

# Should not require edits below this line

> /tmp/java.security.append

# Check for non-v3 CMS provider in java.security.
```

```

if grep CMSProvider $JAVA_HOME/lib/security/java.security >/dev/null; then
  if ! grep -i "CMSProvider V3" $JAVA_HOME/lib/security/java.security; then
    echo "CMS Provider already present, but no 'V3' argument: $JAVA_HOME/lib/security/java.security"
    exit 1
  fi
else
  # Need to add CMSv3 provider.
  # Hunt for the next provider offset
  let NEXT_PROVIDER=1
  for PROVIDER in 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15; do
    if grep security.provider.$PROVIDER $JAVA_HOME/lib/security/java.security >/dev/null; then
      let NEXT_PROVIDER=$NEXT_PROVIDER+1
    fi
  done

  # Stash the provider line in a file
  echo "security.provider.$NEXT_PROVIDER=com.ibm.security.cmskeystore.CMSProvider V3" > /tmp/java.security.append
fi

if [ $# -eq 0 ]; then
  $JAVA_HOME/bin/ikkeycmd -Djava.security.properties=/tmp/java.security.append -help
else
  $JAVA_HOME/bin/ikkeycmd -Djava.security.properties=/tmp/java.security.append "$@"
fi

```

## Setting up auto scaling for Liberty collectives

8.5.5.4

Auto scaling provides an autonomic scaling capability of Liberty servers. The auto scaling functionality is enabled by two Liberty features, scaling controller and scaling member. Auto scaling dynamically adjusts the number of Java virtual machines (JVMs) used to service your workload. This feature provides operational agility and decreases administrative overhead to enhance the resiliency of your middleware environment. The conditions for auto scaling are defined by scaling policies. These conditions include the minimum or maximum number of server instances and the threshold values for each of the server resources.

### Before you begin

This feature does not require the use of Dynamic Routing, however auto scaling performs well when both features are used together. It is recommended to use the two features together. For more information on Dynamic Routing, see “Setting up dynamic routing for Liberty collectives” on page 1493.

Liberty collective controllers can use the Tivoli Remote Execution and Access (RXA) toolkit to perform selected operations on collective members. Review the tasks in “Setting up RXA for Liberty collective operations” on page 1491 to learn more about installing and using SSH.

You must also set your JAVA\_HOME path before setting up auto scaling. Review the tasks in “Setting the JAVA\_HOME variable for Liberty collective members” on page 1147.

### About this task

An auto scaling cluster is a server cluster that can expand and contract depending on the workload in your environment. The Liberty scaling controller controls the starting and stopping of scaling members that are based on performance information that is collected from the scaling members and configurable scaling policies. To be a scaling member of a server cluster, a Liberty scaling controller must also be a member of a Liberty collective. A server cluster has a unique name within a Liberty collective. In Liberty, members of the same server cluster will have the same cluster name, if they are within the same collective. Auto scaling capabilities are controlled by using policies when the consumption of resources rises above an upper threshold or falls below a lower threshold.

The auto scaling functionality is enabled by two Liberty features, scaling controller and scaling member.

- **scalingController-1.0**

The scaling controller feature decides when to expand or contract an auto scaling cluster. Collective controllers are required because they provide administration functionality that leverages the ability of the collective controller to manage the scaling controller. Only one of the running scaling controllers can make decisions. For more information on collective controllers and how to configure your controllers for high availability, see “Configuring a Liberty collective” on page 1136. The scaling controller can start an auto scaling cluster member in response to increased resource usage, or it might stop an auto scaling cluster member in response to decreased resource usage across the entire cluster. If replica sets are being used, all collective controller members must be scaling controllers. When using replica sets if a controller is stopped, another running scaling controller takes over for it. For more information about replica sets, see “Configuring Liberty collective replica sets” on page 1148.

**Note:** The scaling controller keeps the last known state of the scaling members. Stopping the scaling controller and changing the state of the scaling members may cause some invalid actions at the scaling controller restart, until the scaling controller has gathered the latest scaling member state.

The scaling controller supports the following usage scenarios:

- JVM elasticity

The scaling controller starts and stops existing Liberty servers that are based on resource usage and optional scaling policies. There is no provisioning of new servers.

- **8.5.5.7** Liberty elasticity

The scaling controller can install Liberty software onto registered hosts and provision new servers, and then start and stop those servers, based on resource usage and optional scaling policies.

- **scalingMember-1.0**

The scaling member feature monitors the workload within the server and its host, when needed it sends this information back to the scaling controller. The scaling member feature must be enabled as a collective member in a collective.

**Note:** All scaling member servers must also belong to a cluster because all policy information is applied at the cluster member.

If there are two or more scaling members on a host, then the scaling members are organized so that only one scaling member communicates with the scaling controller. The host leader is nominated from among all the scaling members on a host. If the host leader stops, then another scaling member will take over as the host leader.

Each scaling member needs to define a **hostSingleton** element with a port in the `server.xml`. All the scaling members on the same host and cluster must use the same port. This port is used by an election service to identify a host leader. The host leader is the only scaling member that communicates with the scaling controller. The host leader communicates metric data from the members to the controller and communicates scaling decisions that are made by the controller to the members in the host. For example:

```
<hostSingleton name="ScalingMemberSingletonService" port="5164" />
```

For more information about the **hostSingleton** element, see “Collective Member” on page 866.

The scaling member monitors the use of the following resources within the server process:

- CPU
- Heap
- Memory

The scaling member monitors the use of the following resources at the host level:

- CPU
- Memory

## Procedure

1. Create a collective to use for auto scaling.
  - Configure auto-scalable clusters for JVM elasticity.
  - **8.5.5.7** Configure provisionable clusters for Liberty elasticity.
2. Define scaling policies to change the criteria that the scaling controller uses to manage workload. See “Defining scaling policies to manage workload” on page 1511 for more information.

## Results

With the auto scaling feature enabled, you can now dynamically adjust the number of Java virtual machines (JVMs) used to service your workload.

**Note:** The auto scaling cluster capabilities are only available in WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS.

## Configuring auto-scalable clusters for JVM elasticity

**8.5.5.5**

You can configure a collective to support Java virtual machine (JVM) elasticity. With JVM elasticity, the scaling controller can start or stop Liberty servers based on resource use and scaling policies. Only the servers that are already in the collective are eligible for scaling. There is no provisioning of new servers.

### Before you begin

The types of collected resource usage information vary among JDKs. IBM JDK 1.7 for Windows and Linux operating systems provides all necessary usage information for auto scaling and is the preferred JDK. Other JDKs may not provide all necessary usage information for auto scaling based on the individual JVM resource usage.

**Avoid trouble:** The administrative console allows a start and a stop of a Liberty server that is a cluster member of an auto-scalable cluster, but only when the server is in maintenance mode. Starting or stopping a Liberty server from the command line when the Liberty server is a cluster member of an auto-scalable cluster can lead to unpredictable results.

## Procedure

1. Create a collective.

For details on creating a collective controller and member server, see “Configuring a Liberty collective” on page 1136.

**Note:** We recommend that you complete the first step before continuing. Step one instructs the user to create the collective, add members, and start the controllers and members.

2. Add the **scalingController-1.0** feature to the `server.xml` file of one or more collective controllers. When you save the `server.xml` file, default policies will be enforced unless otherwise specified.

```
<featureManager>
  <feature>jsp-2.2</feature>
  <feature>collectiveController-1.0</feature>
  <feature>scalingController-1.0</feature>
</featureManager>
```

After adding the feature, the following messages display in any order in the `messages.log` of the collective controller, provided the collective controller is running:

```
CWWKV0300I: The StackManager service started.
CWWKV0302I: The existing stacks are []
CWWKV0100I: The ScalingController feature is activated.
CWWKX1002I: Singleton service ScalingControllerSingletonService for scope
CWWKV0102I: This server is elected to be the primary scaling controller.
CWWKF0012I: The server installed the following features: [scalingController-1.0].
```

**Note:** Since Liberty configuration is dynamic, when you add the scaling controller, the controller's default scaling policy will take effect and you may get unexpected results. For example, the default policy has `min=2` servers, so when you save the scaling controller `server.xml` file the controller will attempt to start two servers. If you don't want that behavior, you may want to define a policy for the controller at the same time.

**Note:** It might take some time for the scaling controller to register the member and display the `CWWKV0121I` message.

3. Optional: Change the default scaling policies to meet the needs of your environment. Refer to "Defining scaling policies to manage workload" on page 1511 for more information.
4. Add both the **clusterMember-1.0** and **scalingMember-1.0** features to all collective members which you want the scaling controller to control. Define a `hostSingleton` element with a port in the member `server.xml` files. Each scaling member needs to define a `hostSingleton` element with a port in the `server.xml`. All scaling members on the same host must use the same port. You can specify any port number, but the port number must be unique on the host computer. The following example uses port number 20020 :

```
<featureManager>
  <feature>jsp-2.2</feature>
  <feature>clusterMember-1.0</feature>
  <feature>scalingMember-1.0</feature>
</featureManager>
```

```
<hostSingleton name="ScalingMemberSingletonService" port="20020" />
```

If the server is not started when you add the features and the `hostSingleton` element, you must start it manually once for the scaling controller to recognize the added features. The following messages display in any order in the `messages.log` of the collective member:

```
CWWKX1000I: The SingletonMessenger MBean is available.
CWWKX7400I: The ClusterMember MBean is available.
CWWKX1002I: Singleton service ScalingMemberSingletonService for scope host is created.
CWWKV0200I: The ScalingMember feature is activated.
CWWKX1004I: Messenger connection is connected to host=controller_host_name, port=controller_port_number.
```

Only one scaling member per host communicates with the scaling controller. The first scaling member to connect to the **ScalingMemberSingletonService** is elected as the host leader. If the host leader stops, then another scaling member will take over as the host leader via an election process arbitrated by the **scalingMemberSingletonService**. All the scaling members on the same host and cluster must use the same **ScalingMemberSingletonService** port.

**Note:** When a scaling member is elected as the host leader, you will see the following message in the `messages.log` of the collective member:

```
CWWKV0203I: Server host=host_name; userdir=path_to_usr_directory; server=member_name; port=member_port_number; service=
```

**Note:** If you do not add the **hostSingleton** element to the scalingMember `server.xml` or if you use different ports on each scalingMember on the same host, multiple host leaders may be elected. This can result in incorrect scaling decisions. You will see this message in the controller's `messages.log`:

```
CWWKV0123E: Duplicate host singleton leaders have been detected on host host_name. This condition may degrade scaling o
```

For more information about the **hostSingleton** element, see "Collective Member" on page 866.

8.5.5.5



**Watch:** The Configuring a Liberty auto-scalable cluster for JVM elasticity video demonstrates the procedure. [Transcript]

## Configuring provisionable clusters for Liberty elasticity

8.5.5.7

You can configure a collective to support Liberty elasticity. With Liberty elasticity, the scaling controller can install Liberty software onto a registered host and create a new server. Also, because support for Liberty elasticity includes support for JVM elasticity, the scaling controller can start or stop Liberty

servers based on resource use and optional scaling policies. The number of available servers grows when application demand is high and shrinks when application demand is low.

## Before you begin

Determine the target hosts onto which you want to install Liberty software and the Liberty software to install. Minimally, you want the scaling controller to install the following installable and package files on a target host:

- A package that provides a stand-alone Liberty server with one application. Step 5c explains how to create the server package.
- An installable that provides a Liberty server that contains the `wlp` directory, but does not contain the `usr` directory. Step 5a explains how to create the Liberty runtime archive installable.

Each target host needs RXA or SSL and a Java Runtime Environment (JRE) installed that meets the minimum requirements of the Liberty server. See “Setting up RXA for Liberty collective operations” on page 1491 and “Setting the `JAVA_HOME` variable for Liberty collective members” on page 1147.

If a target host does not have a JRE installed with its `JAVA_HOME` variable and System `PATH` variable providing a path to the JRE, the scaling controller can install the JRE on the target host. Step 5b explains how to create a JRE archive, an installable.

 **Watch:** The Configuring an auto-scalable cluster for Liberty elasticity video shows how to configure a provisionable cluster. [Transcript]

## Procedure

1. Configure a collective to support Java virtual machine (JVM) elasticity. Ensure that the collective has at least one dynamic cluster member.

For details on configuring scaling controllers with dynamic cluster members, see “Configuring auto-scalable clusters for JVM elasticity” on page 1505.

2. Ensure that each existing dynamic cluster member belongs to a cluster named with the `StackGroupName.PackageName` naming convention.

Existing dynamic cluster members and servers that the scaling controller will provision will be members of this cluster. `StackGroupName` is the name of a shared directory which will hold installables and packages that a scaling controller will provision to target hosts based on scaling policies. `PackageName` is the name of the server package that the scaling controller will provision to target hosts.

For a cluster named `myStackGroup.cluster1`, put the following statement into the `server.xml` file of each existing dynamic cluster member:

```
<clusterMember name="myStackGroup.cluster1"/>
```

You will use the cluster name for steps 5c and 7 of this topic. In step 5c, use `cluster1.zip` for the server package name. In step 7, create the `myStackGroup` directory for the installables and packages to be deployed.

3. Optional: Add scaling policies to the scaling controller. See Defining scaling policies.
4. Register each target host with a scaling controller.

Registering a host enables the scaling controller to transfer files to that host, as well as access files, commands, and other resources on the host. Use the `registerHost` command to register a target host. Look at the `server.xml` file of the scaling controller to find the values for the `--host`, `--port`, `--user`, and `--password` parameters. To not use an SSH private key file, such as for target hosts on Linux or Windows operating systems, include an operating system login user and password by setting `--rpcUser` and `--rpcUserPassword` parameters. The user specified by `--rpcUser` must have operating system rights to the target deployment location.

```
wlp/bin/collective registerHost targetHost --host=controllerHost --port=controllerHTTPSPort --user=controllerAdmin --password=con
```

To transfer files to target hosts, you do not need to include a `--hostWritePath` parameter in the command; the stack provisioning code sets write paths for you. If a host is already registered, you can use the **updateHost** command to reset registration information. For more information, see “Registering host computers with a Liberty collective” on page 1142.

If the target host is on the same computer as the controller host, you must also run the **updateHost** command for the controller host.

5. Create and configure installables and packages that a scaling controller can deploy onto a registered host.

An *installable* is a binary file the application you want to install on a registered host needs to run, such as a Liberty runtime or JRE. A *package* is that application packaged into a compressed file.

- a. Create a Liberty runtime archive that contains the `wlp` directory, but does not contain the `usr` directory. The naming convention for this installable is *type.name.zip*; for example, `wlp.855.zip`. To create a Liberty runtime archive, you have the following options:

- Run the Liberty server **package** command with the `--include=wlp` option; for example:

```
wlp/bin/server package --include=wlp
```

To specify a file name and target location, add the `--archive=archive_path_name` option; for example:

```
wlp/bin/server package --include=wlp --archive=c:\temp\wlp.855.zip
```

If you do not specify a valid file name or target location with the `--archive` option, then the command creates the `wlp.zip` runtime archive in the `$WLP_OUTPUT_DIR` location, which is the `${wlp.install.dir}/usr/servers` directory by default. The target location must exist before running the command. Thus, if the target location is `c:\temp`, the `C:\temp` directory must exist and have write permission for the command to write the archive to the `C:\temp` directory.

- Run the **package** command with the `--include=all` option and then delete the `usr` directory. The **package** command resembles:

```
wlp/bin/server package myServer --include=all --archive=myArchive.zip
```

- Create a compressed (`.zip`) file that contains the `wlp` directory, without the `usr` directory.

After you create the Liberty runtime archive, ensure that the archive name follows the naming convention, *wlp.name.zip*.

- b. Create or obtain archives for the Java development kit (JDK) and any other required installable. The naming convention for an installable is *type.name.zip*; for example, `jre.17.zip`. Valid type values for installables are:

- `wlp` for a Liberty runtime.
- `jre` for a Java runtime environment.
- `other` for a different file type. This is the default.

For example, to create an archive for a JRE, create a compressed (`.zip`) file that contains the contents of the `java` directory of your IBM JRE installation. Do not include the `java` directory, but include all folders and files in the `java` directory. Follow the *jre.name.zip* naming convention when naming the archive.

- c. Create a server package that contains a Liberty server and applications. The naming convention for a server package is *package\_name.zip*; for example, `cluster1.zip`. Options for creating a server package include:

- Run the **package** command:

```
wlp/bin/server package cluster1 --include=usr
```

The command creates a server package named, for example, `C:\wlp\usr\servers\cluster1\cluster1.zip`.

- Run the **package** command with the `--include=all` option and then delete the `wlp` directory. The **package** command resembles:

```
wlp/bin/server package cluster1 --include=all --archive=cluster1.zip
```

- Create a compressed (`.zip`) file that contains the `usr` directory, without the `wlp` directory.

For example, to create a server package named `cluster1.zip` that consists of a stand-alone Liberty server with one application:

- 1) Create a server:

```
wlp/bin/server create cluster1
```

- 2) Copy an application to the `dropins` directory of the `cluster1` server.

- 3) Package the server:

```
wlp/bin/server package cluster1 --include=usr
```

The `wlp/usr/servers/cluster1/cluster1.zip` file is created.

**Important:** Ensure any `server.env` file in the package has environment settings that are valid on the target hosts. For example, if `JAVA_HOME` is set, it must be set to a location that exists on the target hosts to prevent failed deployments.

**Note:** Windows For Windows target hosts, create a `server.env` file that sets `JAVA_HOME` to the JRE location on the target hosts. After running the **package** command, place the `server.env` in the same directory as the `server.xml` file in the server package ZIP. Example `server.env` contents are:

```
JAVA_HOME=C:\wlp\jre\jre.17.zip\jre
```

6. Set a user name and password for the stack manager in the scaling controller `server.xml` file.

```
<stackManager controllerUser="adminUser" controllerUserPassword="adminPassword" />
```

7. Place the installables and packages in the `WLP_STACK_GROUPS_DIR` location, which by default is `$WLP_USER_DIR/shared/stackGroups`.

Scaling controllers monitor default installable and package locations in the file system and dynamically react to updates. If you place the installables and packages in the default locations, you do not need to change any of the default attributes.

You can use the default stack group, `defaultStackGroup`. Or you can create your own subdirectory of `stackGroups`, such as `myStackGroup`, and add to it the `installables` and `packages` subdirectories.

```
wlp/usr
  /servers
  /shared
  ...
  /stackGroups
    /defaultStackGroup
      /installables
      /packages
    /myStackGroup
      /installables
      /packages
```

The scaling controllers deploy the installables and packages onto the registered host and create a new server.

**Tip:** A new server is created only if the scaling policy is enabled and requires a new server. To force a scaling controller to create a new server, adjust the `min` value and possibly the `max` value of the scaling policy for the scaling controller. For example, if your scaling controller does not have a scaling policy and your collective has three scaling members, add to the scaling controller `server.xml` file a policy that forces the scaling controller to have at least four running members:

```
<scalingDefinitions>
  <defaultScalingPolicy enabled="true" min="4" max="6"/>
</scalingDefinitions>
```

The cluster naming convention for Liberty elasticity is `StackGroupName.PackageName`. When a stack is deployed, `<clusterMember name="StackGroupName.PackageName">` is automatically set in the `server.xml` file of the deployed server. The corresponding `<scalingPolicy>` element includes a `<bind clusters="StackGroupName.PackageName"/>` statement.

Table 109. Default installable and package locations. Liberty environment variables set the default installation directories. To override the default locations, see “Customizing the Liberty environment” on page 1565.

File	Default installation directory
Installable type wlp	/wlp
Installable type jre	/wlp.jre
Installable type other	/wlp.other
Package	/wlp.usr

- Examine the configuration attributes for stack groups and installables and change the configurations of your stack groups and installables as needed to define when and where to run Liberty provisioning. You might need to override the default configurations.

Override default configurations by setting new values in the `stackGroup` and `installable` elements of the scaling controller `server.xml` file. See *Scaling Controller* for information about the `stackGroup` and `installable` elements.

Tips for overriding default values for some elements follow:

- The `installable` element defines an installable for a stack group. The `installable` element can be a child element of the `stackGroup` element or a sibling referenced by an `installableRef` child element of the `stackGroup` element.

**8.5.5.7** The following examples show how you can change the settings in the scaling controller `server.xml` file to override the default value for the `installable` attribute of a stack group:

```
<stackGroup name="myStackGroup">
  <installable name="wlp.v8555.zip" sourceDir="c:\myStackGroup\installables"/>
</stackGroup>
```

or

```
<stackGroup name="myStackGroup" installDir="/myInstallDir" installableRef="myInstallable1, myInstallable2"/>
<installable name="wlp.v8555.zip" id="myInstallable1" sourceDir="c:\myStackGroup\installablesOne" />
<installable name="jre.v1.6.zip" id="myInstallable2" sourceDir="c:\myStackGroup\installablesTwo"/>
```

- The `deployVariable` child element specifies a substitution variable which gets injected into the deployed stack. You can specify that the substitution variable automatically increment each time the stack is deployed. For example, use a `deployVariable` attribute to specify an initial port number value and increment the value each deployment. The purpose of `deployVariable` in this situation is to avoid port conflicts on the target host. The `deployVariable` element uses arithmetic in the `server.xml` file of the deployed server to derive the runtime port number.

For example, to define a starting port value and amount to increment:

- Set `httpPort="{http.port}"` in the `httpEndpoint` element of the packaged server `server.xml` file:

```
<httpEndpoint ... httpPort="{http.port}" />
```

- Add a `deployVariable` definition that sets the starting port and increment values to the scaling controller `server.xml` file:

```
<stackGroup name="DefaultStackGroup" installDir="">
  <deployVariable name="http.port" value="9080" increment="1"/>
</stackGroup>
```

Then, each successive time the stack is deployed to the host, the `httpPort` value increments by 1. Thus, the first time the stack is deployed to `host1`, the HTTP endpoint element is:

```
<httpEndpoint ... httpPort="9080" />
```

and the second time the stack is deployed to `host1`, the element is:

```
<httpEndpoint ... httpPort="9081" />
```

As to the `deployVariable` attribute, the default value for `value` is `null`. The default value for `increment` is 0 (zero).

If `deployVariable` is specified in the scaling controller `server.xml` file, the runtime port number of a deployed server is the initial port value String increased by the increment integer.

- If the scaling controller `server.xml` defines the stack group as follows, do not define `httpPort` again in the `bootstrap.properties` file for the server directory with which you create a server package. If you do, the `httpPort` value defined in `bootstrap.properties` is used, not the one generated by the `deployVariable` configuration element.

```
<stackGroup name="DefaultStackGroup" installDir="">
  <deployVariable name="http.port" value="9080" increment="1"/>
</stackGroup>
```

9. Optional: Change the interval at which the scaling controller checks the file system for stack group additions, updates, and deletions.

The scaling controller scans the contents of the `stackGroups` directory and its subdirectories for changes. Content changes can cause the controller to provision clusters that previously did not have packages available. Updating packages does not cause the controller to provision existing clusters again.

By default, the controller scans the `WLP_STACK_GROUPS_DIR` location every 5000 milliseconds (five seconds). To change the scanning interval or disable scanning, set new values for the stack manager attributes `scanningInterval` and `scanningEnable` in the scaling controller `server.xml` file. For example, to set the scanning interval to six seconds and enable scanning, add a statement resembling the following to the scaling controller `server.xml` file:

```
<stackManager groupsDir="{wlp.install.dir}/usr/shared/stackGroups/"
  controllerUser="adminUser" controllerUserPassword="adminPassword"
  scanningInterval="6000" scanningEnable="true">
</stackManager>
```

To disable scanning, set `scanningEnable` to `false`.

10. Optional: Instruct the scaling controller to scan the file system for new stack group additions, updates, and deletions.

Run a `StackManager` MBean operation to force the scaling controller to check the `WLP_STACK_GROUPS_DIR` location for stack group additions, updates, and deletions. Even if the scaling controller `server.xml` file has `scanningEnable="false"`, you can run a `StackManager` MBean operation to force a scanning for additions, updates, and deletions.

See “Liberty: List of provided MBeans” on page 1647 for information about the `StackManager` MBean.

11. Optional: Start IHS to enable routing to servers.

For IBM HTTP Server (IHS) to discover and route to web applications on dynamically provisioned clusters, enable dynamic routing on the host where the scaling controller will reside. IHS will retrieve the routing information for the provisioned servers from the dynamic routing service. If server status is enabled, you can view the routing information.

If you do not have IHS installed, see “Setting up dynamic routing for Liberty collectives” on page 1493. Also, the following video demonstrates how to install support for dynamic routing using IBM Installation Manager:

 **Watch:** The Enabling IHS for Liberty Dynamic Routing video shows how to install IHS, install Web Server Plug-in for WebSphere Application Server, and apply the interim fix for Dynamic Routing. [Transcript]

## Defining scaling policies to manage workload

8.5.5.4

Scaling policies are used to start and stop dynamic cluster members based on configurable metrics. Scaling Policy can be defined for all or specific clusters. If no policy is defined, a built-in policy will be used.

## About this task

The scaling controller uses scaling policies to make decisions about managing workload. By default, a built-in scaling policy is embedded in the scaling controller. Optionally, you may override the built-in scaling policy by defining either or both top level elements, default scaling policy and scaling policy. The built-in scaling policy is as follows:

- A minimum of two cluster members, if available, are kept active. The minimum number might not be met if some or all of the members are exceeding the metric thresholds.
- An additional cluster member is started when the average CPU, heap, or memory use of all active members exceeds 90%.
- A cluster member is stopped when the average CPU and heap use drops below 30%.

Scaling policy may be defined for all clusters using the default scaling policy. The default scaling policy inherits built-in scaling policy metrics, including `min` and `max` instance values. Any changes made to the default scaling policy, specified by the user, will override the built-in value. Values that are not specified in your default scaling policy will be inherited from the built-in scaling policy.

Unlike default scaling policy, scaling policy metrics are not inherited from either the built-in or default scaling policy. However, `min` and `max` instance values are initialized to the built-in policy values. Because scaling policy metrics are considered optional values, only the metrics specified in the policy are included in scaling decisions. Metrics not included in the scaling policy are not analyzed when making scaling decisions.

There are two levels of scaling policies. You can override the built-in scaling policy by defining either or both top level elements. Here are the two levels that can be defined:

- **Default scaling policy**

You can define a single default scaling policy to manage all clusters that do not need a more specific scaling policy defined.

The following example shows how to define a default scaling policy that sets the minimum number of active cluster members to 3.

```
<scalingDefinitions>
  <defaultScalingPolicy min="3"/>
</scalingDefinitions>
```

- **Scaling policy**

You can define a scaling policy to manage one or more clusters with targeted criteria that is specified in the scaling policy. Because scaling policy definitions do not inherit metric thresholds, only metric thresholds that are specified will be monitored. All other thresholds will be ignored as it relates to scaling decisions. Built-in scaling policy values for `min` and `max` instances will still be respected if they are not specified.

The following example shows how to define a scaling policy that changes the CPU use thresholds for starting and stopping servers in a cluster named `cluster1`.

```
<scalingDefinitions>
  <scalingPolicy id="cluster1Policy">
    <bind clusters="cluster1"/>
    <metric name="CPU" min="10" max="70"/>
  </scalingPolicy>
</scalingDefinitions>
```

The value of the `clusters` attribute of the `bind` element is a comma-separated list of cluster names. An asterisk can be used at the end of the name only as a wildcard to match zero-or-more characters. For example:

```
<bind clusters="west,south*"/>
```

In this example, the scaling policy applies to a cluster named *west* and all clusters whose name starts with *south*. If a cluster name matches multiple policies, the scaling controller uses the following rules to choose a policy:

- An exact match is preferred to a wildcard match.
- If there are multiple wildcard matches, the policy with the longest prefix is used.

The policy will scale based on default min and max values. In the previous example, the clusters will only scale based on the CPU values specified, where min=10 and max=70.

Metric-based scaling decisions are made on a cluster level. Each cluster member monitors its own metrics. The CPU and Memory metric value for a server is actually the greater of the server JVM process or the server's host. The Heap metric value is only taken from the server JVM process. If a measurable change in a monitored metric is detected, that metric is sent to the controller for analysis. All cluster member metrics are accumulated and a cluster average is calculated for each metric. The calculated value for each metric is then compared to the defined upper or lower threshold to determine if a scaling decision will be triggered.

*Scale out* decisions are made on an individual metric basis. All monitored metrics are analyzed for the cluster and if any one of the metrics exceeds the policy max threshold, a scale out event is triggered. *Scale in* decisions are made based on all monitored metrics. The cluster average for each monitored metric is analyzed. If all metrics are below their policy min threshold, a scale in event is triggered.

After a scaling decision is made, the scaling controller selects a scaling target. The scaling target is the host on which the server stop (for scale in) or server start (for scale out) action is run. When determining a target for a scale out action, the host level metrics are taken into consideration. If any of the host level metrics exceed that metric's policy max threshold, the scaling controller avoids that host and chooses another host for the scale out action.

**8.5.5.8** The scaling policy can influence the selection of the scaling target. If the policy specifies `scalingPreference="horizontal"`, the scaling controller starts a server on the eligible host with the fewest active servers and stops a server on the host with the most active servers. If the policy specifies `scalingPreference="vertical"`, the scaling controller starts a server on the eligible host with the most active servers and stops a server on the host with the fewest active servers. The scaling controller attempts to place servers in the same cluster on different hosts when possible, regardless of which `scalingPreference` is chosen.

For more information on **scalingPolicy** metrics see, “Scaling Controller” on page 950.

You can use the **hostGroup** element to limit which hosts can be selected to provision a new server. The `tags` attribute specifies a list of administrative metadata tags. When the scaling controller needs to provision a server, it can only select a host that has at least one matching tag. For example, the policy below says that servers can be provisioned on a host that has *tag1* or a host that has *tag2* associated with it.

```
<scalingDefinitions>
  <scalingPolicy id="provisionPolicy">
    <bind clusters="defaultStackGroup.deployMember"/>
    <hostGroup tags="tag1 tag2"/>
  </scalingPolicy>
</scalingDefinitions>
```

**Note:** If you do not specify the **hostGroup** element, the scaling controller can provision a server on any host that is registered with the collective.

For more information on setting administrative metadata tags see, “Setting administrative metadata for Liberty resources” on page 1476.

## Procedure

1. In the server.xml file of the scaling controller, add the default scaling definitions.

```
<scalingDefinitions>
<defaultScalingPolicy enabled="true" min="1" max="2"/>
</scalingDefinitions>
```

2. When a scaling policy is modified, the server.xml in the controller is also modified. You can check the messages.log file for the following messages to verify that the controller was successfully updated.

```
CWWKG0016I: Starting server configuration update.
CWWKG0028A: Processing included configuration resource: /opt/IBM/Liberty/wlp/usr/
CWWKG0017I: The server configuration was successfully updated in 0.052 seconds
```

You will see the following error messages in the messages.log file if the scaling policy is missing necessary metric thresholds. Follow the user action to correct the error.

```
CWWKV0126W: The configuration of scaling policy {0} does not contain a min or max threshold.
CWWKV0127W: The configuration of scaling policy {0} does not contain a max threshold.
CWWKV0128W: The configuration of scaling policy {0} does not contain a min threshold.
```

## Results

Your scaling policies are now defined.

## Intelligent Management: supported server virtualization environments for CPU metric policy

Before you deploy Intelligent Management on virtualized servers, you must understand the limitations for the server virtualization platform that you are using.

**Remember:** This topic lists the most up to date information on the support of various server virtualization platforms.

Table 110. Server virtualization environments

Virtualization platform	Restrictions	Supported processor sharing mode
AIX 5.3 and AIX 6.1 on POWER5 and POWER6® (Micro-Partitioning®)	None.	Dedicated.
HP-UX 11i v3 on HP using Virtual Partitions (vPars) or Integrity VMs	Currently not supported.	None.
KVM in SUSE Linux Enterprise Server (SLES) 11	Specify 100% affinity to a set of CPU's.	Dedicated.
Linux on POWER® (Micro-Partitioning)	None.	Dedicated.
Linux on z/VM®	None.	Dedicated.
Linux Xen	None.	Dedicated.
Microsoft Hyper-V	Specify 100% affinity to a set of CPU's.	Dedicated.
Solaris Operating Environment 10 on Sun (Zones)	None.	Dedicated.
VMware ESX 3.5, 4.0, 4.1, 5.0 VMware vSphere 4, 5	Guest CPU utilization reporting accuracy is dependent on the following: <ul style="list-style-type: none"> <li>• Guest Operating System</li> <li>• Virtual Machine Reservation</li> <li>• Limit Settings</li> </ul>	Dedicated.

## Deploying scaling policies to a Liberty collective

8.5.5.5

You can use the `scaling-metadata.xml` file to set scaling policies for an auto-scalable cluster. The `scaling-metadata.xml` file uses XML format and does not exist by default. You must create the file and place it in a cluster member configuration directory. After creating the `scaling-metadata.xml` file, you can deploy it through a server package to a Liberty collective.

### Procedure

1. Create an auto-scalable cluster with `<scalingMember metadataMonitorEnabled="true"/>` in its configuration. Optionally, specify a cluster name for the collective member.

The following example defines an auto-scalable cluster member in a cluster named `cluster1`:

```
<featureManager>
  <feature>collectiveMember-1.0</feature>
  <feature>clusterMember-1.0</feature>
  <feature>scalingMember-1.0</feature>
</featureManager>
<clusterMember name="cluster1"/>
<scalingMember metadataMonitorEnabled="true"/>
```

This example changes two default settings:

- The `<clusterMember name="cluster1"/>` statement assigns the member to the `cluster1` cluster. This statement is optional. Without this statement, the cluster member is assigned to `defaultCluster`.
- The `<scalingMember metadataMonitorEnabled="true">` statement enables monitoring for the `scaling-metadata.xml` file. The default is `metadataMonitorEnabled="false"`, which disables monitoring.

Optionally, you can omit `<feature>clusterMember-1.0</feature>` from the auto-scalable cluster configuration because the `scalingMember-1.0` feature enables the `clusterMember-1.0` feature. The `clusterMember-1.0` feature is shown in this example for clarity.

For information about creating an auto-scalable cluster, see “Configuring auto-scalable clusters for JVM elasticity” on page 1505.

2. Create a text file named `scaling-metadata.xml` that defines a scaling policy.

```
<?xml version="1.0" encoding="UTF-8" ?>
<server description="Scaling Policy for cluster1">
  <scalingDefinitions>
    <scalingPolicy name="cluster1">
      ...
      <bind clusters="cluster1"/>
    </scalingPolicy>
  </scalingDefinitions>
</server>
```

The `bind` element must specify the name of the cluster to be deployed in a server package. In this example, the `bind` element specifies `cluster1`. If your cluster member definition does not specify a cluster name, specify `defaultCluster`.

3. Place the `scaling-metadata.xml` file in the cluster member configuration directory.

The directory is `${wlp.install.dir}/usr/servers/cluster_member_name` or, if the `$WLP_USER_DIR` variable is set in a `server.env` file or command window, `$WLP_USER_DIR/servers/cluster_member_name`.

The product deploys the scaling policy to the collective repository when the following events occur:

- The cluster member connects with the controller, such as when the cluster member starts
- The `clusterMember` feature name attribute changes
- The `scaling-metadata.xml` file changes for the cluster member

The product monitors the `scaling-metadata.xml` file after the cluster member starts and dynamically deploys any file changes to the collective repository. If the cluster member is removed from the collective controller through the collective remove command, the product undeploys the scaling policy from the collective repository.

4. Optional: Package the cluster member into a server package and deploy the package.

- a. Package the cluster member into a server package.

Available tools for packaging archives include:

- The Liberty server **package** command. Sample command syntax is:

```
wlp/bin/server package cluster_member_name --include=all | minify --archive=cluster_member_name.zip | jar | pax
```

- The **package** action in the WebSphere Developer Tools for Eclipse product.

For example, to use the package command:

- 1) Stop the cluster member if it is running.
- 2) Run the **package** command to create the server package. For example, if the cluster member name is clusterMember1, run:

```
wlp/bin/server package clusterMember1
```

The command creates a server package named, for example, C:\wlp\usr\servers\clusterMember1\clusterMember1.zip on Windows computers.

You might need to customize the installation by changing port numbers, database connections, or messaging system connections.

- b. Deploy the server package to host computers.

Available tools for deploying packages include:

- Deploy tool of Admin Center
- FileTransfer MBean
- Server package deployment through DevOps, such as Chef. For information about DevOps, see the WASdev website.
- Server package manual deployment
- Change to deployed server

## Entering maintenance mode for Liberty collectives

8.5.5.7

Enter maintenance mode before you perform diagnostic tests, maintenance, or tuning, on a host or server. Maintenance mode can prevent the disruption of client requests by routing client traffic around a server that is in maintenance mode, to another server.

### About this task

When a server that is a scaling member is in maintenance mode, the scaling controller cannot start or stop that server. The server does not count toward the minimum or maximum running instance settings for the cluster.

**Note:** To achieve the full advantages of using maintenance mode in a Liberty collective, it is recommended that you enable the dynamic routing feature, auto scaling feature, or both of these features. For more information about the dynamic routing and auto scaling features, see “Setting up dynamic routing for Liberty collectives” on page 1493 and “Setting up auto scaling for Liberty collectives” on page 1503.

When a host is in maintenance mode, the scaling controller cannot provision a new server on that host.

You can enter maintenance mode on a server that is joined to a collective or on a host that is registered to a collective.

You can use maintenance mode to alter the routing of requests by a web server that is enabled for Intelligent Management.

Entering a server or a host into maintenance mode is a persistent change. A server or host remains in maintenance mode even if the server is restarted until the mode is explicitly changed.

## Procedure

1. Use the collective **enterMaintenanceMode** command to place a server or a host and its servers into maintenance mode.

```
wlp/bin/collective enterMaintenanceMode
  --host=controllerHostName
  --port=controllerHttpsPortNumber
  --user=adminUser
  --password=adminPassword
  --hostName=serverHostName
  [--usrDir=serverUserDirectory]
  [--server=serverName]
  [--break]
  [--force]
```

The `--host` and `--port` arguments identify which collective controller can process the command. The `--user` and `--password` arguments are the administrative user ID and password for authenticating with the controller.

The `--hostName`, `--usrDir`, and `--server` arguments identify the server to be placed into maintenance mode. If you want to place a host and its servers into maintenance mode, provide the `--hostName` argument only and omit the `--usrDir` and `--server` arguments.

By default, the web server continues to send requests with affinity to a server in maintenance mode. Use `--break` to stop any traffic from being routed to the server, including requests with affinity to the server.

The scaling controller starts another server to replace each scaling member that is placed into maintenance mode. Another server will be started to meet the minimum number of instances of the cluster or to meet current workload demand. By default, if the scaling controller cannot find another server to act as a replacement the server is not placed into maintenance mode. Use the `--force` argument to cause a server to be placed into maintenance mode even if no replacement server is available.

2. Use the collective **exitMaintenanceMode** command to take a server or a host and its servers out of maintenance mode.

```
wlp/bin/collective exitMaintenanceMode
  --host=controllerHostName
  --port=controllerHttpsPortNumber
  --user=adminUser
  --password=adminPassword
  --hostName=serverHostName
  [--usrDir=serverUserDirectory]
  [--server=serverName]
```

3. Use the collective **getMaintenanceMode** command to display whether a server or a host and its servers are in maintenance mode.

```
wlp/bin/collective getMaintenanceMode
  --host=controllerHostName
  --port=controllerHttpsPortNumber
  --user=adminUser
  --password=adminPassword
  --hostName=serverHostName
  [--usrDir=serverUserDirectory]
  [--server=serverName]
```

## Example

In this example, the **hostc** has a collective controller. The collective controller has the scaling controller and dynamic routing features enabled. In the `server.xml` file of the scaling controller, the minimum number of active cluster members is set to 1. **Host1** has two started cluster members, *memberA1* for *cluster A* and *memberB1* for *cluster B*. **Host2** has one stopped cluster member, *memberA2* for *cluster A*. All cluster members have the scaling member feature enabled. A web server that is enabled for Intelligent Management also exists, which is routing requests to the cluster members.

To put **host1** into maintenance mode, enter the following command:

```
wlp/bin/collective enterMaintenanceMode
--host=hostc
--port=controller1HttpsPortNumber
--user=adminUser
--password=adminPassword
--hostName=host1
```

The command issues the following response:

Successfully enter maintenance mode for host1.

An alternate server must be started. Maintenance mode will be set for memberA1 when the alternate server is started. Could not enter maintenance mode for memberB1 because an alternate server is not available.

The scaling controller starts *memberA2* as a replacement for *memberA1*. After *memberA2* is started, then *memberA1* is placed into maintenance mode. The web server no longer routes HTTP requests to *memberA1*.

The scaling controller cannot replace *memberB1*, therefore the member is not placed into maintenance mode. You can run the command again by using the `--force` argument to force *memberB1* to be placed into maintenance mode, which can affect the performance of the requests running in *clusterB*.

## What to do next

The health controller also uses server maintenance mode as an action that is taken when the health policy is breached. For example, if you are using an excessive response time condition, and the response time exceeds the specified average response time threshold for a server, then the server can move to maintenance mode.

## Maintenance mode

8.5.5.7

The maintenance mode feature allows a host or server to be taken offline without disrupting service. Maintenance mode works with the dynamic routing and auto scaling features to prevent the disruption of client requests by routing client traffic that is targeted for a server that is in maintenance mode, to another server. Enter maintenance mode before you perform diagnostic tests, maintenance, or tuning, on a host or server.

### Server maintenance mode

- A server in maintenance mode is not included in the count of active servers in an auto scaled cluster.
- When a server is in maintenance mode the dynamic routing feature routes requests to other servers in the collective.

### Host maintenance mode

- All servers on the host are entered in to maintenance mode when the host is placed in maintenance mode.
- All servers move out of maintenance mode when a host is taken out of maintenance mode.
- A host in maintenance mode makes that host unavailable for provisioning a new Liberty instance.
- Any server on a host in maintenance mode may be individually taken out of maintenance mode while a host remains in maintenance mode.

## Maintenance mode collective command options

Maintenance mode is controlled by an administrator by using the collective command. This command is expanded to include syntax for entering or exiting maintenance mode.

## Command Syntax

- `collective enterMaintenanceMode [options]`
- `collective exitMaintenanceMode [options]`
- `collective getMaintenanceMode [options]`

## Base collective command options

### **--host="controller host name"**

Required – Name of the host on which the collective controller resides.

### **--port="controller HTTPS port"**

Required – Specifies the HTTPS port number of the target collective controller.

### **--user="user"**

Required – The administrative user of the target collective controller.

### **--password="password"**

Required – The administrative user's password.

## Maintenance mode specific options

### **--hostName="target Host Name"**

Required – The name of the host going into maintenance mode or the host that contains the server going into maintenance mode.

### **--usrDir="Liberty installation directory"**

Required for Server – The root directory where Liberty is installed on the host.

### **--server="server Name"**

Required for Server – The name of the server being placed into maintenance mode

### **--break**

Applies to `enterMaintenanceMode` only.

When not specified the default is to stop new traffic to the server, but allow traffic with affinity to continue to use the server that has entered maintenance mode. When `--break` is specified all requests are routed to another server.

### **--force**

Applies to `enterMaintenanceMode` only.

When `--force` is specified, the server will be forced to enter maintenance mode even if an auto scaling policy will be violated.

## Configuring health management for Liberty

8.5.5.7

Health management in a Liberty collective can prevent the disruption of service by detecting common problems and generating diagnostic actions based on configured health policies. The health management functions are enabled by two Liberty features, health manager and health analyzer.

### Before you begin

- Create the environment that you want to monitor. When creating a health policy, have in mind the target of the policy (server, cluster or host).
- If you want to gain the full functionality of the health management feature, it is recommended that both the auto scaling and dynamic routing features be enabled. For more information, see “Setting up auto scaling for Liberty collectives” on page 1503 and “Setting up dynamic routing for Liberty collectives” on page 1493.

- The types of collected resource usage information varies among JRE/JDKs. Go to <http://www.ibm.com/developerworks/java/jdk/index.html> on the developerWorks website and download an IBM JRE/JDK for your operating system. The developerWorks website does not have a JRE for all operating systems. For example, you must get the JDK from Eclipse for Windows operating systems. The following IBM Java versions for Windows and Linux operating systems provide all necessary usage information and are the preferred JRE/JDKs.
  - Java 8
  - Java 7 Fix Pack 8 and above
  - Java 6 Fix Pack 7 and above

**Note:** Health Center generates temporary tmp files in the /tmp space, and depending on /tmp space limits, you might want to change the java.io.tmpdir to avoid filling the /tmp space, which can cause unrecoverable issues on some platforms.

```
-Djava.io.tmpdir=/path/to/tmpdir
```

**Note:** Windows For Windows users, the root user does not have read/write permission to the C:\Windows\Temp directory unless you are an administrator. You might want to change the permission of the C:\Windows\Temp directory to avoid this issue.

## About this task

You can create health policies for common server health conditions. For more information, see “Health management” on page 1521.

You can also assign the following actions for health conditions:

- Capture diagnostics (heap dump and thread dump)
- Restart server
- Enter server into maintenance mode
- Exit server out of maintenance mode. For use within the same health policy, where an earlier action entered maintenance mode prior to performing other actions.

 **Watch:** Video: Health management for Liberty collectives provides an overview of health management and demonstrates how it can help find and mitigate problems in your Liberty applications. [Transcript]

## Procedure

1. Create a collective. For details on creating a collective controller and member server, see “Configuring a Liberty collective” on page 1136.
2. Add the healthManager-1.0 feature to the feature manager stanza in the server.xml file of one or more collective controllers. This feature can only be added to collective controllers.

```
<featureManager>
  <feature>jsp-2.2</feature>
  <feature>collectiveController-1.0</feature>
  <feature>healthManager-1.0</feature>
</featureManager>
```

After you add the feature, the following message in the messages.log file of the collective controller, provided the collective controller is running,

```
CWWKV0600I: The HealthManager feature is activated.
```

3. Add the `healthAnalyzer-1.0` feature to the feature manager stanza of the `server.xml` file of the collective member. The `healthAnalyzer` feature is necessary for monitoring excessive memory usage and memory leak.

```
<featureManager>
  <feature>collectiveMember-1.0</feature>
  <feature>healthAnalyzer-1.0</feature>
</featureManager>
```

After you add the feature, the following message displays in the `messages.log` file of the collective controller, provided the collective controller is running.

```
CWKKV0750I: The healthAnalyzer feature has been activated.
```

When the `healthAnalyzer` feature is activated on the collective member, the following message displays in the `messages.log` file of the collective controller.

```
CWKKV0612I: The Health Analyzer is activated in member_host_name,path_to_usr_directory,member_name.
```

**Note:** If you want to activate both the `healthAnalyzer` and `scalingMember` features, the `hostSingleton` specification must have a unique port separately set for each service .

```
<hostSingleton name="ScalingMemberSingletonService" port="33333">
<hostSingleton name="HealthAnalyzerSingletonService" port="33334">
```

4. If you want to target clusters, you must also configure the collective members to be a part of a server cluster.

For more information about server clusters, see “Setting up Liberty server clusters” on page 1153.

5. Add one or more `healthPolicy` elements to the `server.xml` file of the collective controller. Each `healthPolicy` element defines a single health policy. If more than one policy is needed, multiple health policy elements can be added to the `server.xml` file. For more information about adding `healthPolicy` elements to the `server.xml` file, see “Health management policies for Liberty” on page 1523.

## Results

With health policies enabled, Intelligent Management can monitor collective members for problems, and perform diagnostic actions.

## Health management

8.5.5.7

With the health management feature in Liberty, you can take a policy-driven approach to monitoring the application server environment and take action when unhealthy criteria is discovered.

You can define the health policies, which include the health conditions to be monitored in your environment and the health actions to take if these conditions are met.

### Health conditions

Health conditions define the variables that you want to monitor in your environment. The condition element defines what behavior can trigger this health policy. Only one condition element can be defined per health policy. You can choose from the following predefined health conditions:

#### Excessive request timeout condition

Specifies a percentage of HTTP requests that can time out. When the percentage of requests exceeds the defined value, the health actions run. The timeout value depends on your environment configuration.

```
<excessiveRequestTimeout timeoutPercentage="5"/>
```

**Note:** Dynamic Routing must be enabled to use this condition.

### Excessive response time condition

Tracks the average amount of time that requests take to complete. If the time exceeds the defined response time threshold, the health actions run.

```
<excessiveResponseTime responseTime="10s"/>
```

**Note:** Requests that exceed the timeout value that is configured for the excessive request timeout condition are not counted towards this health condition. For example, if the default timeout value is set to 60 seconds, then any request that exceeds 60 seconds will time out and is not included in the average response time calculation for this health condition. This restriction applies even if you do not have an excessive request timeout condition defined.

**Note:** Dynamic Routing must be enabled in to use this condition.

### Memory condition: excessive memory usage

Tracks the memory usage for a member. When the memory usage exceeds a percentage of the heap size for a specified time, health actions run.

```
<excessiveMemoryUsage heapSizePercentage="85" timePeriod="5m"/>
```

### Memory condition: memory leak

When a downward trend in free memory is detected, health actions run.

```
<memoryLeak/>
```

## Health actions

Health actions define the activities to perform when a health condition is not met. Action elements define what action will be taken in response to a detected condition. All actions share the element type of `<action>`. The action attribute determines which action is taken and multiple actions can be defined for each health policy. Actions are run in the order they are specified in the policy. The following table lists the health actions that are supported in Liberty server environments:

Table 111. Predefined health action support for Liberty servers

Health action	Liberty servers that run in the same collective controller
Restart server	Supported
Take thread dumps	Supported
Take Java virtual machine (JVM) heap dumps	Supported for servers that are running on the IBM JRE or JDK
Enter server into maintenance mode	Supported
Exit server out of maintenance mode	Supported

```
<action action="generateThreadDump"/>  
<action action="generateHeapDump"/>  
<action action="restartServer"/>  
<action action="enterMaintenanceMode"/>  
<action action="exitMaintenanceMode"/>
```

## Health targets

Target elements define the scope of the topology that is being monitored for the condition. There are three target types:

- A host  

```
<host hostName="someHost"/>
```
- Each of the servers in a cluster  

```
<cluster clusterName="someCluster"/>
```
- A single-server

```
<server hostName="Host" wlpUsrDirectory="/opt/ibm/liberty/wlp" serverName="Server"/>
```

Each target type has a unique element that is used to define it within the `healthPolicy` element. More than one target can be specified per health policy.

## Health management policies for Liberty

8.5.5.7

You can define the health policies, which include the health conditions that you want to monitor in your environment and the health actions to take if these conditions are met.

### About this task

Health policies are configured in the same manner as other Liberty features. Within the `server.xml` file configuration, a new element type of `<healthPolicy>` is used to define a single health policy. If more than one policy is needed, multiple health policy elements can be added to the `server.xml` file.

### Procedure

1. Insert the health policy into the `server.xml` file and provide an identity for the health policy.
2. Add the desired target elements to the health policy stanza in the `server.xml` file.

**Note:** More than one target can be specified per health policy.

3. Specify the condition that is being monitored within the health policy stanza.

**Note:** Only one condition per policy is allowed.

4. Specify the actions within the health policy stanza.

**Note:** You can specify more than one action per health policy. If more than one action is specified, the actions are run in the order they are defined in the policy.

For more information about health policy target elements, see “Health management” on page 1521.

### Example

In this example, the health policy specifies that all servers in cluster `mycluster1` and all servers on host `myHost` are monitored for excessive memory usage. The policy monitors the `excessiveMemoryUsage` condition based on the specified thresholds. The policy instructs the health management controller to place the server experiencing the excessive memory usage into maintenance mode and request a heap dump from that server.

```
<healthPolicy id="myHealthPolicy" >
  <cluster clusterName="mycluster1"/>
  <host hostName="myHost"/>
  <excessiveMemoryUsage heapSizePercentage="85" timePeriod="5m"/>
  <action action="enterMaintenanceMode"/>
  <action action="generateHeapDump"/>
</healthPolicy>
```

When a health policy is added, the following messages display in any order in the `messages.log` file of the collective controller.

```
CWWKV0609I: The health policy myHealthPolicy is added.
```

```
CWWKV0603I: The health condition com.ibm.ws.health.manager.healthPolicy.condition.excessiveMemoryUsage is being monitored
```

```
CWWKV0607I: The health policy myHealthPolicy is activated for member_host_name,path_to_usr_directory,member_name.
```

**Note:** Messages CWWKV0603I and CWWKV0607I display when there is at least one member server in the collective that is identified in a target element.

When a health policy is modified, the following messages display in any order in the `messages.log` file of the collective controller.

```
CWWKV0610I: The health policy myHealthPolicy is removed.
```

```
CWWKV0604I: The health condition com.ibm.ws.health.manager.healthPolicy.condition.excessiveMemoryUsage is no longer being m
```

```
CWWKV0609I: The health policy myHealthPolicy is added.
```

```
CWWKV0603I: The health condition com.ibm.ws.health.manager.healthPolicy.condition.excessiveMemoryUsage is being monitored o
```

## Liberty collective troubleshooting

### 8.5.5.0

There are a number of common issues you might encounter when troubleshooting Liberty. As to collectives, the issues typically relate to configuration of the collective controller, member, or host system. Browse the list of issues to learn how to resolve the issues.

- Issues involving connection
  - “CWWKO0801E: Unable to initialize SSL connection. Unauthorized access was denied or security settings have expired.”
  - CWWKX0217E: No MBean is currently registered with the given *object\_name*
  - CWWKX0215E: There was a problem with the user name or password provided
  - CWWKX8057I: The collective member is unable to establish a connection to any of the collective controllers. Configured controllers: [*host\_name:port\_number*]
  - Error: Connection refused: connect
  - `java.net.SocketException` error
- Issues involving **start** and **stop** commands
  - Starting or stopping the servers remotely causes a Java not found error
  - CTGRI0000E: Could not establish a connection to the target machine with the authorization credentials that were provided
  - CTGRI0001E: The application could not establish a connection to *host\_name*
  - **8.5.5.4** CTGRI0026E A connection could not be completed to *host\_name* during the specified timeout interval
  - CWWKX6027E: The collective controller initialization did not succeed. The socket bind did not succeed for host *host\_name* and port *port\_number*. The port might already be in use or the host does not match the system configuration.
  - CWWKX7204E: Cannot connect to host *host\_name* with the credentials provided

For fixes to other issues, see “Liberty:Runtime environment known issues and restrictions” on page 2333.

## Issues involving connection

**CWWKO0801E: Unable to initialize SSL connection. Unauthorized access was denied or security settings have expired.**

Message:

```
CWWK00801E: Unable to initialize SSL connection.  
Unauthorized access was denied or security settings have expired.  
Exception is javax.net.ssl.SSLHandshakeException:  
Client requested protocol TLSv1 not enabled or not supported
```

Cause:

TLSv1.2 security might be improperly configured for a collective controller and its member servers. The members cannot communicate with the controller.

Ensure the `server.xml` file for the controller and each member has `ssl id` elements for the TLSv1.2 SSL protocol; for example:

```
<ssl id="defaultSSLConfig"  
    sslProtocol="TLSv1.2"  
    keyStoreRef="defaultKeyStore"  
    trustStoreRef="defaultTrustStore"  
    clientAuthenticationSupported="true" />
```

```
<ssl id="controllerConnectionConfig"
    sslProtocol="TLSv1.2"/>

<ssl id="memberConnectionConfig"
    sslProtocol="TLSv1.2"/>
```

To enable members to communicate with the controller, you might also need to add an `etc` directory to the main Liberty installation directory on each host and add a `server.env` file to the `${wlp.install.dir}/etc` directory. Ensure the `server.env` file has the following content:

```
JVM_ARGS=-Dhttps.protocols=TLSv1.2
```

See “Setting up Liberty to run in SP800-131a” on page 1848.

#### **CWWKX0217E: No MBean is currently registered with the given *object\_name***

Message:

```
Error: CWWKX0217E: No MBean is currently registered with the given ObjectName 'WebSphere:feature=collectiveController,type=Collect
```

Cause:

The MBean might not be available yet. Check the server logs to see if the MBean has reported ready.

There might have been a problem starting the collective repository. Check to see if the collective repository has started.

If the target is a collective controller, verify that the replica set is active. If a majority of the collective controller replicas are not started, this message will be seen. Start the remaining replicas.

The servers configuration might be incomplete. Make sure that the server is properly configured.

#### **CWWKX0215E: There was a problem with the user name or password provided.**

Message:

```
Error: CWWKX0215E: There was a problem with the user name or password provided. The server responded with code 401 and message 'Un
```

Cause:

The username and password might be incorrect. Make sure that the username and password are correct for the target server.

The user might not be granted the Administrator role. Make sure that the user is granted the Administrative role, or choose a different user.

The security configuration for the target server might be incomplete. Make sure that the security configuration is defined and the security service reports as ready (CWWKS0008I).

#### **| CWWKX8057I: The collective member is unable to establish a connection to any of the collective | controllers. Configured controllers: [host\_name:port\_number]**

Message:

```
CWWKX8057I: The collective member is unable to establish a connection to any of the collective controllers. Configured controllers
```

Cause:

The servers might not be running. Verify that the collective controller and member servers are running.

If the servers are running, determine whether the SSL configuration in the `server.xml` of the controller or a member changed recently. If this CWWKX8057I message occurs in the member, then the controller is more likely to have an incorrect SSL configuration. If this message occurs in the controller, then a member is more likely to have an incorrect SSL configuration. The problem can occur when a configuration does not use a `quickStartSecurity` element.

To fix a problem with the SSL configuration, check the following in the `server.xml` file:

1. Ensure the administrator role is configured. “Mapping the administrator role for Liberty” on page 1644 compares `quickStartSecurity` element settings to those for basic or LDAP registry.
2. Review and update the SSL configuration as needed.

- a. Check any default SSL configuration. Look for `<sslDefault sslRef="LDAPSSLSettings"></sslDefault>` to see if the `server.xml` file contains a default configuration and to see if it is necessary to specify one SSL configuration as the default.

If the `<sslDefault sslRef="LDAPSSLSettings"></sslDefault>` configuration is not necessary, remove it so the configuration has two or more SSL configurations (for example, one for the collective, one for LDAP) to use.

If the default configuration is necessary, keep the `<sslDefault sslRef="LDAPSSLSettings"></sslDefault>` line and proceed to steps b and c to add client authentication and import certificates to the default SSL configuration. See “Configuring LDAP user registries in Liberty” on page 1852.

- b. Enable client authentication. Configure the HTTPS port for the server with `clientAuthenticationSupported="true"`.

For example, a collective controller that uses LDAP SSL default for security must have `clientAuthenticationSupported="true"` in its `ssl` element to work with a collective member.

- c. Import necessary certificates. You can use `keytool` to import certificates. The default truststore must include certificates from `collectiveTrust.jks`.

Background information:

By default, `<sslDefault sslRef>` points to `defaultSSLSettings`. Changing `<sslDefault sslRef>` in the collective controller configuration to point to something other than `defaultSSLSettings`, such as `<sslDefault sslRef="LDAPSSLSettings"/>`, causes the CWWKX8057I error unless the configuration has `clientAuthenticationSupported="true"` and the Liberty server trusts any SSL peer that has a client certificate.

SSL settings for HTTPS must trust the collective certificates. Changing `<sslDefault sslRef>` to point to something other than `defaultSSLSettings` without `clientAuthenticationSupported="true"` can unbind the `defaultSSLSettings` from their HTTPS configuration. The collective SSL settings are part of the default configuration.

For more information, see “Mapping the administrator role for Liberty” on page 1644, “Configuring LDAP user registries in Liberty” on page 1852, and “Configuring an `httpEndpoint` to use an SSL configuration other than the default” on page 1850.

#### **Error: Connection refused: connect**

Message:

Error: Connection refused: connect

Cause:

The host and port might be incorrect. Make sure that the host and port are correct for the target server.

The server might not be running. Make sure that the server is running.

#### **java.net.SocketException error**

Message:

java.net.SocketException: java.security.NoSuchAlgorithmException: Error constructing implementation (algorithm: Default, provider: Su

Cause:

The truststore and truststore password might be incorrect. Make sure that the truststore path, truststore password, and contents of the truststore are correct.

## Issues involving start and stop commands

### Starting or stopping the servers remotely causes a Java not found error

Message:

Starting or stopping the servers remotely (using **ClusterManager.startCluster** or **ServerCommands.startServer** for example) encounters the following error:

```
{stderr=java: javaCmd 14: serverCmd 32: ./server 873: FSUM7351 not found, stdout=, returnCode=127}
```

Solution:

The member servers need a `server.env` file that specifies a `JAVA_HOME` variable.

### CTGRI0000E: Could not establish a connection to the target machine with the authorization credentials that were provided.

Message:

```
CTGRI0000E Could not establish a connection to the target machine with the authorization credentials that were provided.
```

Cause:

Authentication fails using user name or password:

- Make sure that the user name and password are correct in the target server's `server.xml` `<hostAuthConfig>` element.
- Update the host authentication configuration using the collective **updateHost** command.

Authentication fails using ssh keys:

- Check permissions on:
  - `~/ssh` should be `0700`
  - `~/ssh/authorized_keys` should be `0600`
- `~/ssh` and all children must be correct if using SELinux. Use **restorecon -R** to fix the permissions.

### CTGRI0001E: The application could not establish a connection to *host\_name*.

Message:

```
{ExceptionMessage=ConnectException caught while performing stopCluster operation on member webpla.ibm.com,/P1A/WebSphere_LP/usr,me  
CTGRI0001E The application could not establish a connection to webpla.ibm.com., Exception=java.net.ConnectException: CTGRI0001E Th
```

Cause:

Starting or stopping the servers remotely using commands such as **ClusterManager.startCluster** or **ServerCommands.startServer** can cause the error.

**8.5.5.4** Message CTGRI0001E, along with message CTGRI0026E, can indicate that too many concurrent SSH connections are made to a host. Possible causes are:

- Autonomics such as scaling controller
- Running **ClusterManager.startCluster**, **ServerCommands.startServer**, or other system management commands on a number of servers on a single host that exceeds the maximum number of concurrent unauthenticated connections to the SSH daemon.

Solution:

Confirm that the RPC mechanism (such as SSH) is started. Also confirm that the configured settings, such as host and port, are correct.

**8.5.5.4** If your environment uses SSH, change the settings in the SSH configuration file. The SSH configuration `MaxStartups` setting has a default of 10 concurrent unauthenticated connections. Changing the `MaxStartups` setting in the SSH configuration file,

`/etc/ssh/sshd_config`, can solve the problem. The `MaxStartups` setting specifies the maximum number of concurrent unauthenticated connections to the SSH daemon. Additional connections are dropped until authentication succeeds or the `LoginGraceTime` expires for a connection. You can enable random early drop by specifying the three colon separated values `start:rate:full` (for example, `10:30:60`). `sshd(8)` refuses connection attempts with a probability of `rate/100` (30%) if there are currently `start` (10) unauthenticated connections. The probability increases linearly and all connection attempts are refused if the number of unauthenticated connections reaches `full` (60). The following sample SSH configuration file settings specify `MaxStartups` and other settings that can alleviate connection problems:

```
ClientAliveInterval 60
ClientAliveCountMax 3
MaxSessions 100
MaxStartups 100:30:200
LoginGraceTime 180
```

For more information about Secure Shell (SSH) protocol and changing `/etc/ssh/sshd_config` settings, see “Setting up RXA for Liberty collective operations” on page 1491.

**8.5.5.4 CTGRI0026E A connection could not be completed to `host_name` during the specified timeout interval.**

Message:

```
CTGRI0026E A connection could not be completed to webpla.ibm.com during the specified timeout interval.
```

Cause:

Too many concurrent SSH connections to a host can cause this error.Solution:

See the solution for message CTGRI0001E.

**CWWKX6027E: The collective controller initialization did not succeed. The socket bind did not succeed for host `host_name` and port `port_number`. The port might already be in use or the host does not match the system configuration.**

Message:

```
CWWKX6027E: The collective controller initialization did not succeed. The socket bind did not succeed for host * and port 10,010. The
```

Solution:

Ensure that the host value specified in the collective controller configuration is correct. For example, if the collective controller resides on `myhost.com`, check the `server.xml` file of the controller to ensure the host value is correct:

```
<variable name="defaultHostName" value="myhost.com" />
```

The example message shows an asterisk (\*) for host, suggesting that the host value probably did not cause the problem. The likely cause of the problem is a port conflict.

Ensure that the port number in the message is not already in use. At a command line on the host computer where the collective controller resides, run `netstat -a` to see a list of port numbers and the status of the connections. If the port number is in use, the list contains an entry such as the following for port 10,010:

```
TCP 127.0.0.1:10010 myhost:0 LISTENING
```

To fix this port conflict, open an editor on the `server.xml` file of the collective controller and add a statement that sets `replicaPort` to a port number that is not in use on the computer. Any of the following statements can set a `replicaPort` value:

- `<collectiveController replicaPort="10011"/>`
- `<collectiveController replicaHost="myhost.com" replicaPort="10011"/>`
- `<collectiveController replicaPort="{prop.controller_1.replica}"/>`

Set the variable for the port number, which has the name `prop.controller_1.replica` in this statement but which can have any variable name you choose, in a `bootstrap.properties` file or in a `<variable name="name" value="value"/>` XML tag.

#### **CWWKX7204E: Cannot connect to host *host\_name* with the credentials provided.**

Message:

```
localhost,C:/wlp,member1 stop operation resulted in an Exception: ConnectException caught while performing stopCluster operation o
CWWKX7204E: Cannot connect to host localhost with the credentials provided.
```

Solution:

Make sure that the cluster member authentication information is set correctly and that all Remote Execution and Access (RXA) requirements are met. Many RXA operations require access to resources that are not generally accessible by standard user accounts. See “Setting up RXA for Liberty collective operations” on page 1491 for more information.

---

## Setting up a Liberty server to use Bluemix services

8.5.5.9

You can configure a Liberty server to use Bluemix services. Not all Bluemix services are available for configuration.

### bluemixUtility command

8.5.5.9

Use the IBM Bluemix command-line utility to configure your on-premises Liberty server to use certain Bluemix cloud services.

#### Sources

Learn about Bluemix services, such as Watson and Cloudant® services, that you can use with the command-line utility.

- To register for or log in to a Bluemix account, see [Sign up for IBM Bluemix](#).
- To learn more about Watson, see [Watson services](#).
- To learn more about Cloudant services, see [Getting started with Cloudant NoSQL DB](#).

#### Syntax

The command syntax is as follows:

```
bluemixUtility action [options]
```

Use the following *action* commands:

**login** Log in to Bluemix. If you run the **login** command without any options, the tool prompts you for more information, such as username and password. After a successful login, Bluemix credentials are saved to a file so that you can run other commands without specifying username and password again.

If you log in to Bluemix with the Cloud Foundry (cf) client, the `bluemixUtility` uses the credentials saved by the `cf` client. For more information, see [Cloud Foundry \(cf\) commands](#).

#### **marketplace**

List all the Bluemix services that can be configured by using the command-line utility.

#### **createService**

Create a service instance from the Bluemix catalog.

**listServices**

List all the available Bluemix service instances.

**showService**

Show information about a service instance.

**import**

Import a configuration for a service. The imported service configuration and its dependencies are placed in the following directory:

```
`${wlp.user.dir}/shared/config/services/serviceName
```

**listImports**

List all imported service configurations that can be bound to a Liberty server.

**bind**

Bind a Bluemix service configuration to a Liberty server. The configuration for a service may provide default values for certain options, such as the `jndiName` of a `dataSource` element. In some cases, the default values do not match what the application expects. Use the `--v` option to override a default value with the value that your application expects.

**unbind**

Unbind a service configuration from a Liberty server.

**deleteService**

Delete a service instance.

**switch** Switch to a different Bluemix organization or space.

**info** View Bluemix connection information.

**help** Use the help action on each command to view descriptions, usage, and options.

**logout** Log out of Bluemix. The **logout** command deletes the file that was created when you logged in with Bluemix credentials.

## Usage

View usage examples that you can run for each action.

Use the following command to run the **login** action:

```
bluemixUtility login [options]
```

Use the following command to run the **marketplace** action:

```
bluemixUtility marketplace [serviceType...]
```

Use the following command to run the **createService** action:

```
bluemixUtility createService [options] serviceType servicePlan serviceName
```

Use the following command to run the **listServices** action:

```
bluemixUtility listServices
```

Use the following command to run the **showService** action:

```
bluemixUtility showService [options] serviceName
```

Use the following command to run the **import** action:

```
bluemixUtility import [options] serviceName
```

Use the following command to run the **listImports** action:

```
bluemixUtility listImports [serverName]
```

Use the following command to run the **bind** action:

```
bluemixUtility bind [options] serverName serviceName
```

Use the following command to run the **unbind** action:

```
bluemixUtility unbind serverName serviceName
```

Use the following command to run the **deleteService** action:

```
bluemixUtility deleteService [options] serviceName
```

Use the following command to run the **switch** action:

```
bluemixUtility switch [options]
```

Use the following command to run the **logout** action:

```
bluemixUtility logout
```

## Options

View the available options for each action.

The following options are available for the **bluemixUtility login** command:

### **--api=url**

Bluemix API endpoint, for example, `https://api.ng.bluemix.net`. The API endpoint can also be set as the Bluemix region name. For example, it can be set to `us-south` for the US South region, `eu-gb` for the London, UK region, and `au-syd` for the Sydney, Australia region.

### **--user=username**

User name of Bluemix account.

### **--password=password**

Password of Bluemix account.

### **--org=organizationName**

Organization name.

### **--space=spaceName**

Space name.

The following options are available for the **bluemixUtility marketplace** command:

### **[serviceType...]**

Show detailed information about a particular Bluemix service. Specify multiple service names by separating them with a space.

The following options are available for the **bluemixUtility createService** command:

### **--credentialName=name**

The name of the service credential. By default, `credential-1` is used.

### **serviceType**

The type of service to create.

### **servicePlan**

The name of service plan.

### **serviceName**

The name of service to create.

No options are available for the **bluemixUtility listServices** command.

The following options are available for the **bluemixUtility showService** command:

**--showCredentials**  
Display service credentials.

**serviceName**  
The name of a Bluemix service.

The following options are available for the **bluemixUtility import** command:

**--acceptLicense**  
Automatically indicate acceptance of license terms and conditions.

**--credentialName=name**  
The name of the service credential. By default, the first credential that is found is used.

**--encodeAlgorithm=[xor|aes]**  
Specifies how to encode sensitive information in the imported service configuration. Supported encodings values are **xor** and **aes**. The default encoding algorithm is **xor**.

**--encodeKey=key**  
Specifies the key to be used when you are encoding with AES encryption. If this option is not provided, a default key is used.

**--p[parameter]=value**  
Specifies parameters that help in generating and importing a configuration for a service.

**serviceName**  
The name of a Bluemix service.

The following options are available for the **bluemixUtility listImports** command:

**[serverName]**  
List the services that are already bound to this particular server.

The following options are available for the **bluemixUtility bind** command:

**--v[variable]=value**  
Override variables in the imported service configuration.

**--acceptLicense**  
Automatically indicate acceptance of license terms and conditions.

**serverName**  
Name of the server to bind to the service configuration.

**serviceName**  
Name of the imported service configuration.

The following options are available for the **bluemixUtility unbind** command:

**serverName**  
Name of the server to unbind the service configuration from.

**serviceName**  
Name of the service configuration to unbind.

The following options are available for the **bluemixUtility deleteService** command:

**--force** Force deletion without confirmation.

**serviceName**  
Name of the service to delete.

The following options are available for the **bluemixUtility switch** command:

**--org=organizationName**  
Organization name.

**--space=spaceName**  
Space name.

No options are available for the **bluemixUtility info** command.

No options are available for the **bluemixUtility logout** command.

## Return codes

Table 112. Return codes and explanations

Return code	Explanation
0	The command successfully completed the requested operation.
20	One or more command-line arguments or options are not valid.
21	An unknown runtime exception has occurred.
22	An IO error occurred, typically when trying to delete a file from the file system.
24	User abort. Occurs when user fails to respond to a prompt or cancels the operation.
26	An unknown exception has occurred.
27	Bluemix authentication error when attempting to log in, or attempting to perform a task without being logged in.
28	A generic error when communicating with Bluemix.
29	A generic error when communicating with the configuration service.
30	A generic service configuration error has occurred.
31	A generic feature installation error has occurred.
255	An unknown error has occurred.

## Configuring Liberty for Bluemix Cloudant services

8.5.5.9

Use the IBM Bluemix utility command-line integration tool to configure your Liberty server to use the Bluemix Cloudant service.

### Before you begin

Before you configure your Liberty server to use Bluemix services, you must create an account. See Sign up for IBM Bluemix to create your Bluemix account.

### About this task

Configure your Liberty server to use the Cloudant service. For more information about Cloudant, see Getting started with Cloudant NoSQL DB.

## Procedure

1. Log in using the **bluemixUtility login** command. After your initial login, you do not have to complete this step again.
2. Run the **bluemixUtility marketplace** command to list details about all the Bluemix services that can be used with the command-line utility. See the following example:

Service: cloudbantNoSQLDB

Description: Cloudant NoSQL DB is a fully managed data layer designed for modern web and mobile applications that leverage Cloudant is built upon and compatible with Apache CouchDB and accessible through a secure HTTPS API, which scales as you Cloudant is ISO27001 and SOC2 Type 1 certified, and all data is stored in triplicate across separate physical nodes in a Documentation: <https://console.ng.bluemix.net/docs/#services/Cloudant/index.html#Cloudant>  
Plans: Standard, Lite

3.

**Note:** If you already created an instance, skip to step 4. You can also create an instance from the Bluemix dashboard.

Run the `bluemixUtility createService [options] serviceType servicePlan serviceName` command to create an instance of the Bluemix services that you want to use. See the following example and description of a service listed:

```
bluemixUtility createService cloudbantNoSQLDB Lite myCloudantService
```

4. Optional: Run the **bluemixUtility listServices** command to view the Name, Type, and Plan of all the services instances that you created. See the following example:

```
myCloudantService cloudbantNoSQLDB Lite
```

5. Run the **bluemixUtility import myCloudantService --pversion=v2** command to import the configuration.

**Important:** The `--pversion=v2` option installs the `cloudbant-1.0` feature and downloads the official Cloudant library for Java. For API information, see the official Cloudant Java library API documentation. If you omit the `--pversion=v2` option, the `couchdb-1.0` feature is installed and Ektorp libraries are used instead to communicate with the Cloudant instance.

- a. Accept the license terms and conditions of the necessary libraries that are needed to access the service.
- b. After the configuration is successfully imported, complete any additional steps to use the imported configuration in your application, such as adding a classloader reference to the library. For example, you must add the following classloader reference to your application to use the downloaded libraries.

```
<application id="myCloudantApp">  
    <classloader commonLibraryRef="cloudbantNoSQLDB-library"/>  
</application>
```

6. Optional: Run the **bluemixUtility listImports** command to view the service configurations that you imported.

The following IBM Bluemix service configurations have been imported:  
myCloudantService

7. Run the `bluemixUtility bind [options] serverName serviceName` to bind the configuration to a Liberty server. Accept the license terms and conditions, if you are prompted. See the following example and description of a service listed:

```
bluemixUtility bind defaultServer myCloudantService
```

Checking if features required for the myCloudantService are installed.  
All required features are installed.  
The myCloudantService is now bound to defaultServer server.

If you imported the service with the `--pversion=v2` option to use the official Cloudant Java libraries, the default JNDI name for the Cloudant database is `cloudbant/serviceName`. If you did not specify that option, the default JNDI name is `couchdb/serviceName`. If your application references the database by using a different JNDI name, use `--vjndiName` option to specify the JNDI name.

```
$ bluemixUtility bind defaultServer myCloudantService --vjndiName=couchdb/connector
```

## Results

You can now use Cloudant services with your Liberty server.

## Configuring Liberty for Bluemix Watson services

8.5.5.9

Use the IBM Bluemix utility command-line integration tool to configure your on-premise Liberty server to use Bluemix Watson services.

### Before you begin

Before you configure your Liberty server to any Bluemix service, you must create an account. See

Sign up for IBM Bluemix to create your Bluemix account.

### About this task

Configure your Liberty server to use Watson services. Your application must use the Watson Developer Cloud Java SDK to access the Watson service. For more information, see [Watson Developer Cloud Java SDK services](#). For more information about Watson, see [Watson services](#).

### Procedure

1. Log in using the **bluemixUtility login** command. After you initially log in, you do not have to complete this step again.
2. Run the **bluemixUtility marketplace** command to list details about all the Bluemix services that can be used with the command-line utility. See the following example of the Concept Insights description:

```
Service: personality_insights
```

```
Description: The Watson Personality Insights derives insights from transactional and social media data to identify ps
```

```
Documentation: https://www.ibm.com/watson/developercloud/personality-insights.html
```

```
Plans: tiered, premium
```

3.

**Note:** If you already created an instance, skip to step 4. You can also create an instance from the Bluemix dashboard.

Run the `bluemixUtility createService [options] serviceType servicePlan serviceName` command to create an instance of the service that you want to use. You can choose a unique `serviceName` for your service instance. The following example creates an instance of the Personality Insights service:

```
bluemixUtility createService personality_insights premium myWatsonService
```

4. Optional: Run the **bluemixUtility listServices** command to view the Name, Type, and Plan of all the service instances that you created. See the following example:

```
myWatsonService personality_insights premium
```

5. Run the **bluemixUtility import myWatsonService** command to import the configuration.
  - a. Accept the license terms and conditions of the necessary libraries that are needed to access the service.
  - b. After the configuration is successfully imported, complete any additional steps to use the imported configuration in your application, such as adding a classloader reference to the library. The classloader element must be added to each application that is using the service. The classloader reference ID is different from each unique Watson service. For example, you must add the following classloader reference to your application to use the Watson Java SDK libraries.

```
<application id="myWatsonApp">
  <classloader commonLibraryRef="personality_insights-library"/>
</application>
```

- Optional: Run the **bluemixUtility listImports** command to view the service configurations that you imported.

The following IBM Bluemix service configurations have been imported:  
myWatsonService

- Run the **bluemixUtility bind** *[options] serverName serviceName* to bind the configuration to a Liberty server. See the following example and description of a service listed:

```
bluemixUtility bind defaultServer myWatsonService
```

Checking if features required for the myWatsonService are installed.

All required features are installed.

The myWatsonService is now bound to defaultServer server.

## Results

You can now use Watson services with your Liberty server.

---

## Setting up a Liberty Server for use with z/OS Connect

z/OS



8.5.5.2

### Setting up z/OS Connect

The z/OS Connect feature runs in a WebSphere Application Server for z/OS, Liberty environment and is installed from the Liberty Repository.

#### Before you begin

8.5.5.2

Use IBM Installation Manager to install Liberty for WebSphere Application Server Version 8.5.5.2, along with the following interim fixes:

- 8.5.5.2-WS-WLP-OS390-IFPI18279
- 8.5.5.2-WS-WLP-OS390-IFPI18379

Download the interim fixes from IBM Fix Central, or install the interim fixes directly from the service repository.

8.5.5.3

Use IBM Installation Manager to install Liberty for WebSphere Application Server version 8.5.5.3 or later.

Use the **featureManager** command for Liberty to install the z/OS Connect feature from the Liberty Repository. This command requires that the file system for Liberty have read/write access. You can either enable the Liberty file system as read/write, or copy the contents into a read/write file system so new features can be added from the Liberty Repository.

#### Procedure

- Change to the **bin** subdirectory under the directory where Liberty is installed. The directory must be enabled for read/write access.

```
cd ${wlp.install.dir}/bin
```

- Use the **featureManager** command to install the z/OS Connect feature:

```
featureManager install zosConnect-1.0
```

The feature is downloaded from the online Liberty Repository and installed. You must have Internet access to retrieve the feature from the Liberty Repository.

3. **8.5.5.2** If you are installing this feature on to Liberty version 8.5.5.2, set the required file permissions by issuing the following commands from the WebSphere Liberty installation directory:  
`chmod ugo+rx bin/zosConnect/bbgls2js` and `chmod ugo+rx bin/zosConnect/bbgjs21s`
4. You are now ready to add the z/OS Connect feature to the feature manager list in the `server.xml` file of the Liberty server where you want to enable this support.

```
<server description="z/OS Connect Liberty Server">
  <featureManager>
    <feature> zosConnect-1.0 </feature>
  </featureManager>
</server>
```

5. (Optional)

- a. If you are using WebSphere optimized local adapters (WOLA), use the **featureManager** command to install the Optimized Local Adapters feature:

```
featureManager install zosLocalAdapters-1.0
```

For more information, see “Installing Liberty Repository assets” on page 1391.

The feature is downloaded from the Liberty Repository and installed. You must have Internet access to retrieve the feature from the Liberty Repository.

- b. Update the `server.xml` file to enable WOLA for outbound calls from your Liberty server to your applications with an external address space.
  - Add a `zosLocalAdapters` element that defines the three-part WOLA group name that is used by clients to connect to the Liberty server.
  - Add a connection factory element and provide a JNDI name. For more information, see the documentation on enabling the Liberty server environment to use optimized local adapters.

```
<server>
  <featureManager>
    <feature>zosConnect-1.0</feature>
    <feature>zosLocalAdapters-1.0</feature>
  </featureManager>

  <!-- Local adapters connection factory definition -->
  <authData id="cauth1" user="user1" password="{xor}LDo8Ki02KyY="/>
  <connectionFactory id="wolaCF" jndiName="eis/ola" containerAuthDataRef="cauth1" >
    <properties.ola/>
  </connectionFactory>

  <!-- Provide WOLA server identity -->
  <zosLocalAdapters wolaGroup="LIB1" wolaName2="LIB2" wolaName3="LIB3" />
</server>
```

## Results

You are now ready to add z/OS Connect service elements to your `server.xml` configuration.

## Defining z/OS Connect services



z/OS<sup>®</sup> Connect service definitions provide the mechanism for reaching z/OS application assets using REST calls. To enable z/OS Connect services, you must add a z/OS Connect service definition to the Liberty `server.xml` file with the element name `zosConnectService` along with a name and service provider reference element name.

### About this task

z/OS Connect services are defined by the `zosConnectService` configuration element. This element contains attribute definitions that may have globally defined counterparts. Attributes can be defined

globally through the `zosConnectManager` element. These attributes, if defined, apply to all services. If both global and service level attributes are configured, the values defined at the `zosConnectService` level are used.

z/OS Connect provides a service implementation that allows z/OS Connect requests to interact with z/OS assets through WebSphere Optimized Local Adapters (WOLA). The service is automatically enabled when both `zosConnect-1.0` and the `zosLocalAdapters-1.0` features are configured. Instances of this service can be defined through the `localAdaptersConnectService` configuration element.

z/OS Connect also provides a service implementation that allows z/OS Connect requests to contact a remote REST endpoints. The service is available when the `zosConnect-1.2` feature is configured. Instances of this service can be defined through the `zosConnectServiceRestClient` configuration element. For more information, see the documentation for the z/OS Connect REST Client Service.

## Procedure

1. Add a `zosConnectService` element for each service in your `server.xml` configuration. You must configure the `serviceRef` and `serviceName` attributes at minimum. The `serviceRef` element points to the service provider configuration element. The `serviceName` attribute is how the service provider identifies itself with z/OS Connect and is also the name to use as part of the URL for z/OS Connect requests that are targeted to a specific service. The service name must be unique. The following is a sample `server.xml` file that shows what is required to add a z/OS Connect service called `recordOpsCreate`:

```
<!-- z/OS Connect service definitions -->
<zosConnectService id="zcs1"
  serviceName="recordOpsCreate"
  serviceRef="wolaCreateService"/>
```

For more information about the configurable attribute definitions associated with the `zosConnectService` element, see the documentation for the z/OS Connect feature.

2. (Optional) Add the `zosConnectManager` configuration element to the `server.xml` file. This element is a singleton in the `server.xml` configuration and it contains global values that apply to all z/OS Connect services that are defined for the server. The element can contain the names of z/OS Connect interceptors or data transformation provider configuration elements that apply to all services in the server.

The following example describes a `zosConnectManager` element that defines an operations group name of `Operator1` under the item `globalOperationsGroup`. This is the name of the security (SAF or LDAP) group that the requesting client `userid` needs to be in before z/OS Connect operations requests are permitted, such as `action=start|stop|status`. This group applies to all services in the z/OS Connect configurations. The item `dataxform` defines the element name where z/OS Connect will find a data transformation provider. Supplying the `dataxform` in the `zosConnect` element means this is the transformation provider implementation for all services in the configuration that do not already have their own data transformation element reference. The `interceptors` item is the name of the element in the configuration that describes the set of z/OS Connect interceptors that apply to all services in the configuration.

```
<zosConnectManager id="zosConnectGlobals"
  globalOperationsGroup="Operator1"
  globalDataxformRef="XformJSON2Byte"
  globalInterceptorsRef="GlobalInterceptors"/>
```

For more information about the configurable attribute definitions associated with the `zosConnectManager` element, see the documentation for the z/OS Connect feature. For more information on each attribute, see the Liberty features documentation.

3. If WOLA is configured in Liberty, the configuration for a request requires a `localAdaptersConnectService` element in the `server.xml` file. This configuration consists minimally of the target WOLA Connection Factory name, Register name and Service name. Configuration of z/OS Connect follows the Liberty conventions by only requiring the minimum parameters to be specified.

Note, when you configure a WOLA connection factory for z/OS Connect interaction, you must use container as the authentication mechanism. WOLA connection factories that do not specify a containerAuthDataRef attribute are not supported. The following is an example:

```
<!-- Local adapters connection factory definition -->
<authData id="cauth1" user="user1" password="{xor}LDo8Ki02KyY="/>
<connectionFactory id="wolaCF" jndiName="eis/ola"
  containerAuthDataRef="cauth1" >
  <properties.ola/>
</connectionFactory>

<!-- Local adapters config -->
<zosLocalAdapters wolaGroup="LIBERTY" wolaName2="LIBERTY"
  wolaName3="LIBERTY" />

<!-- WOLA Connect service and z/OS Connect service definitions -->
<localAdaptersConnectService id="wolaOpsCreate"
  registerName="BATCH01"
  serviceName="COBLPGM1"
  connectionFactoryRef="wolaCF"/>

<zosConnectService id="zcs1" serviceName="recordOpsCreate"
  serviceRef="wolaOpsCreate"
  runGlobalInterceptors="true"
  interceptorsRef="serviceInterceptorList"/>
```

The z/OS Connect service implementation that allows z/OS Connect requests to interact with z/OS assets through WebSphere Optimized Local Adapters (WOLA) might require a data transformer. If a data transformer is configured, globally or at the service level, input and output payloads are converted using the configured data transformer. If a data transformer is not configured, and the request contains a JSON payload, the service assumes that the backend program will handle the data conversion. The service converts the JSON payload, as is, to a byte array using the encoding specified in the request header or the default JSON encoding of UTF-8. Similarly, if the asset returns a payload and no data transformer is configured, the WOLA service implementation expects to receive a JSON payload in byte array form, which is converted to a JSON response payload following the same encoding rules used for transforming a JSON request payload to a byte array.

The WOLA service provider implementation allows for a number of other WOLA connection factory definitions to be specified in its localAdaptersConnectService configuration element. The following table is a list of localAdaptersConnectService attribute definitions and a description of each.

Attribute Definition	Description
serviceName required="true" type="String"	Name of the WOLA target service. This service name must match the name an external address space application is using for the service name on a WOLA Receive Request or Host Service API call, or the program name used for SVC with a WOLA CICS Link Server.
registerName required="true" type="String"	Name of the WOLA target registration. This target registration must match the name an external address space application is using for the register name on a WOLA Register API call, or the name used for RGN with a WOLA CICS Link Server.
connectionFactoryRef required="true" type="String"	Name of the connection factory element with the JNDI name of the WOLA resource adapter connection factory to be used. Refer to the Liberty WOLA resource adapter documentation for more information.

Attribute Definition	Description
connectionWaitTimeout required="false" type="Integer" min="0" max="2147483647"	Number of seconds to wait for an external address space application that matches the registration name to issue a WOLA Receive Request or Host Service API and become active. Refer to the Liberty WOLA resource adapter documentation for more information.
linkTaskTranID required="false" type="String"	Specifies the name of the WOLA CICS Link Server link invocation task transaction ID. Refer to the Liberty WOLA resource adapter documentation for more information.
useCICSContainer required="false" type="Boolean" default="false"	When using the WOLA CICS Link Server, indicates whether the payload is passed in a single CICS container or a COMMAREA to the target CICS application program. Refer to the Liberty WOLA resource adapter documentation for more information.
linkTaskReqContID required="false" type="String"	When using the WOLA CICS Link Server and the useCICSContainer flag is set to true, specifies the name of the target CICS request container. Refer to the Liberty WOLA resource adapter documentation for more information.
linkTaskReqContType type="Integer" min="0" default="0"	When using the WOLA CICS Link Server and the useCICSContainer flag is set to true, specifies the type of the target CICS request container (0=CHAR, 1=BIT). Refer to the Liberty WOLA resource adapter documentation for more information.
linkTaskRspContID required="false" type="String"	When using the WOLA CICS Link Server and the useCICSContainer flag is set to true, specifies the name of the target CICS response container. Refer to the Liberty WOLA resource adapter documentation for more information.
linkTaskRspContType type="Integer" min="0" default="0"	When using the WOLA CICS Link Server and the useCICSContainer flag is set to true, specifies the type of the target CICS response container (0=CHAR, 1=BIT). Refer to the Liberty WOLA resource adapter documentation for more information.
linkTaskChanID required="false" type="String"	When using the WOLA CICS Link Server, specifies the CICS channel name to use for delivering messages and received response messages using CICS containers. Refer to the Liberty WOLA resource adapter documentation for more information.
linkTaskChanType required="false" type="Integer" min="0" default="0"	When using the WOLA CICS Link Server and specifying the linkTaskChanID channel name, specifies the type of the target CICS containers that are associated with that channel (0=CHAR, 1=BIT). Refer to the Liberty WOLA resource adapter documentation for more information.

## Setting up the z/OS Connect REST client service

8.5.5.7

The z/OS Connect REST Client support enables z/OS Connect users to route requests to remote REST applications through z/OS Connect, thereby taking advantage of the existing interceptor infrastructure.

### About this task

This function is available when you configure the `zosConnect-1.2` feature. The z/OS Connect REST Client service is a z/OS Connect service SPI implementation. Requests that invoke this service are made in two ways:

- Use the `?action=invoke` query parameter mechanism as follows: `https://hostName:port/zosConnect/services/serviceY?action=invoke` where `serviceY` is the service name that is associated with the configured `zosConnectServiceRestClient` element.
- Use the `zosConnectService` attribute definition that is called `invokeURI`. You can use this attribute to define a custom URI that is associated with a service name and any of the following HTTP verbs: GET, POST, PUT, DELETE; for example:

```
<zosConnectService serviceName="serviceY" serviceRef="restClientServiceY" invokeURI="/my/custom/uri" />
```

An example of a service invocation for the defined service is: `https://host:port/my/custom/uri` (HTTP verb: GET/POST/PUT/DELETE). z/OS Connect understands the association between the `invokeURI` attribute and the `serviceName` attribute defined in the example. z/OS Connect calls the `invoke` method on the implementation of the z/OS Connect associated service (`restClientServiceY`).

For more information on the capability and flexibility that the `invokeURI` attribute offers, see the documentation for z/OS Connect

### Procedure

1. Configure the `zosConnectServiceRestClient` element and associate it with a `zosConnectService` element.

```
<featureManager>
  <feature>zosConnect-1.2</feature>
</featureManager>

<!-- Global interceptor definition to run for all service requests -->
<zosConnectInterceptors interceptorRef="auth,audit,fileSystemLogger" id="globalInterceptorList1"/>
<fileSystemLoggerInterceptor id="fileSystemLogger" logName="service1Log_%SERVERNAME%" sequence="1"/>
<authorizationInterceptor id="auth" sequence="2"/>
<auditInterceptor id="audit" sequence="3"/>

<!-- ZosConnectManager definition -->
<zosConnectManager globalAdminGroup="ADMIN"
  globalOperationsGroup="OPS"
  globalInvokeGroup="INVOKE"
  globalInterceptorsRef="globalInterceptorList1"/>

<zosConnectServiceRestClient id="restClientServiceY"
  host="remoteHostName"
  port="8800"
  uri="/remote/endpoint"
  httpMethod="DELETE"/>
<zosConnectService serviceName="serviceY" serviceRef="restClientServiceY" invokeURI="/my/custom/uri" />
```

In the example, requests that target the `serviceY` service are routed to the remote host and port that is configured under the associated `restClientServiceY` service and that uses the configured URI and DELETE HTTP method. The JSON payload is automatically sent with the remote request. When you configure the `zosConnectServiceRestClient` element, specify the host name and port number

attributes. If you do not specify the uri or httpMethod attributes, the values that are used are the ones from the original client request that is targeting the serviceY service. The example also shows that because interceptors are configured to run globally, every request that targets the serviceY service is logged, authorized, and audited before it is routed to the remote endpoint. The interceptors also log and audit the responses on the return from the remote endpoint. Because an invokeURI attribute is configured for the serviceY service, the requester can start the implementation of the serviceY invoke method by using the following URL: https://host:port/my/custom/uri and using either the GET, POST, PUT, or DELETE HTTP method. In this case, because the serviceY service refers to an instance of the z/OS Connect REST client service, the invoke() method on this instance is called. For more information about available configuration attributes and default values see the documentation for z/OS Connect 1.0 and z/OS Connect 1.2.

2. (Optional) Configure basic authentication. Add the appSecurity-2.0 feature to the server.xml file.

```
<featureManager>
  <feature>zosConnect-1.2</feature>
  <feature>appSecurity-2.0</feature>
</featureManager>

<zosConnectServiceRestClientBasicAuth id="fredBasicAuth" userName="Fred" password="{xor}0S060y8o0w==" />

<zosConnectServiceRestClient id="restClientServiceY"
  host="remoteHostName"
  port="8800"
  uri="/remote/endpoint"
  httpMethod="POST"
  basicAuthRef="bobBasicAuth"/>

<zosConnectService serviceName="serviceY" serviceRef="restClientServiceY" />
```

The configuration enables the user name and password that is configured for the zosConnectServiceRestClientBasicAuth element to be propagated when the request to the remote REST application endpoint is made.

3. (Optional) Configure certificate authentication. Add the appSecurity-2.0 feature to the server.xml file.

The example shows how to configure the client keystore and client truststore and associate them with the zosConnectServiceRestClient configuration.

```
<featureManager>
  <feature>zosConnect-1.2</feature>
  <feature>appSecurity-2.0</feature>
</featureManager>

<keyStore id="clientKeyStore" password="zosConnect"
  location="{server.config.dir}/resources/security/clientKey.jks" />

<keyStore id="clientTrustStore" password="zosConnect"
  location="{server.config.dir}/resources/security/clientTrust.jks" />

<ssl id="sslCertificates" keyStoreRef="clientKeyStore" trustStoreRef="clientTrustStore"/>

<zosConnectServiceRestClient id="restClientServiceY"
  host="remoteHostName"
  port="8800"
  uri="/remote/endpoint"
  httpMethod="PUT"
  sslCertsRef="sslCertificates"/>

<zosConnectService serviceName="serviceY" serviceRef="restClientServiceY" />
```

## Defining z/OS Connect interceptors



8.5.5.2

z/OS® Connect provides a framework that enables interceptors, or methods, to work with operations such as service invoke, status, start, or stop. Interceptors are OSGi services that implement the `com.ibm.wsspi.zos.connect.Interceptor Service Provider Interface (SPI)` that is provided by z/OS Connect.

## About this task

You can use interceptors for various purposes. z/OS Connect has no visibility into what an interceptor is used for. For example, an interceptor might be written to perform some infrastructure setup that is based on the message payload before the request is processed. z/OS Connect provides a copy of the input request payload to all interceptors.

z/OS Connect provides the `<zosConnectService>` configuration element that enables the administrator to configure a set of attributes that apply to a particular service. One of these attributes is `interceptorsRef`, which points to a configuration element that lists one or more interceptors to run for a specific service.

This task describes how to define a z/OS Connect interceptor and a list of interceptors and also explains how to associate the interceptors with one or more services in the configuration for a server. This task also includes a description of how to enable the z/OS Connect-provided audit and authorization interceptors for services.

## Procedure

1. Update the `<zosConnectService>` element for each service in your `server.xml` configuration for which you want to enable an interceptor or list of interceptors for.

```
<!--z/OS Connect service definitions -->
<zosConnectService id="zcs1"
  serviceName="recordOpsCreate"
  serviceRef="wola0psCreateService"
  interceptorsRef="opsCreateInterceptorList"/>
```

2. Create the associated `<zosConnectInterceptors>` element.

```
<!-- User Interceptor definitions -->
<usr_userInterceptorOne id="userI1" sequence="1"/>
<usr_userInterceptorTwo id="userI2" sequence="2"/>

<zosConnectInterceptors id="opsCreateInterceptorList" interceptorRef="userI1, userI2"/>
```

The name of the interceptor list in this example is `greetingsInterceptorList`. There are two interceptors referred to here, `userI1` and `userI2`. Interceptor implementations use the Liberty SPI extensions. These interceptors must define their metatypes to the Liberty server and create an implementation of the `com.ibm.wsspi.zos.connect.Interceptor` class. In this example, an implementation of this class was created with a metatype that defines the elements `usr_userInterceptorOne` and `usr_userInterceptorTwo`. The name of the configuration element where the list of interceptors is provided is called `interceptorsRef`. It is not a required attribute.

3. Optional: Create a global interceptor list and enable it in the `<zosConnectManager>` element. The `globalInterceptorsRef` item is the name of the element in the configuration that describes the set of z/OS Connect interceptors that apply to all of the services in the configuration.

```
<zosConnectManager id="zosConnectGlobals" globalInterceptorsRef="GlobalInterceptors"/>

<!-- User Interceptor definitions -->
<usr_userInterceptorOne id="userI1" sequence="1"/>
<usr_userInterceptorTwo id="userI2" sequence="2"/>
<zosConnectInterceptors id="globalInterceptors" interceptorRef="userI1, userI2"/>
```

4. Optional: Enable the z/OS Connect-provided audit, authorization, or logging interceptors for a service or set of services. The z/OS Connect-supplied audit interceptor implements the `com.ibm.wsspi.zos.connect.Interceptor` SPI to store audit or tracking information in the z/OS System Management Facility (SMF) data sets. The authorization interceptor provides the ability to verify that the current authenticated user has the authority to perform the requested action. Examples

of actions checked include service action=invoke, start, or stop. You enable these interceptors for one or more services in the z/OS Connect server configuration. The following example shows how to enable both the audit and authorization interceptors for a single service:

```
<!-- z/OS Connect service definition -->
<zosConnectService id="zcs1"
  serviceName="recordOpsCreate"
  serviceRef="wo1a0psCreateService"
  interceptorsRef="opsCreateInterceptorList1"/>

<!-- Audit and authorization interceptor definitions -->
<authorizationInterceptor id="authInterceptor1" sequence="1"/>
<auditInterceptor id="auditInterceptor1" sequence="2"/>

<zosConnectInterceptors id="opsCreateInterceptorList1" interceptorRef="auditInterceptor1, authInterceptor1"/>
```

## Setting up the z/OS Connect file system logger interceptor

8.5.5.7

The file system logger interceptor enables z/OS Connect users to log request information in a file system file.

### About this task

This function is available when you configure the zosConnect-1.0 or zosConnect-1.2 features and it requires configuration.

Table 113. Descriptions of the entries that are in the generated log file

Entry	Description
DateTime	The date and time that is calculated by the logger interceptor before the service invocation
ThreadID	The ID of the thread under which the service request is being processed
UserName	The user name for which the request is being processed
RequestID	The request tracking ID that is generated by z/OS Connect
RemoteAddress	The Internet Protocol (IP) address of the client who originated the request or last proxy that sent the request
LocalAddress	The Internet Protocol (IP) address of the interface on which the request was received
MessageType	Identifies whether the payload is from a request or a response
MessageSize	The character size of the payload
MessageData	A request or response payload

```
*****
ServerName: com.ibm.ws.zos.connect.interceptor.logger.fs
*****
DateTime:2015-07-19_12-14-02 | ThreadId:47 | UserName:Fred | RequestID:0000000000000001000000000000000000000000 |
RemoteAddress:127.0.0.1 | LocalAddress:127.0.0.1
MessageType:REQUEST
MessageSize:27
MessageData:{"payload":"HELLO_SERVICE"}

DateTime:2015-07-19_12-14-02 | ThreadId:47 | UserName:Fred | RequestID:0000000000000001000000000000000000000000 |
```

RemoteAddress:127.0.0.1 | LocalAddress:127.0.0.1  
MessageType:RESPONSE  
MessageSize:26  
MessageData:{"payload":"HELLO\_CALLER"}

## Procedure

1. Configure the `fileSystemLoggerInterceptor` element globally.

```
<fileSystemLoggerInterceptor id="globalFileSystemLogger" logName="globalLog_%SERVERNAME%"/>  
<zOsConnectInterceptors id="globalInterceptorList" interceptorRef="globalFileSystemLogger" />  
<zOsConnectManager globalInterceptorsRef="globalInterceptorList"/>
```

In the example, all z/OS Connect service requests are logged in a file that is called `globalLog_myServer1_yyyy-MM-dd_HH_mm_ss_SSS.log` where `myServer1` is the name of the server. The only required configuration element is the `logName` attribute definition. The configuration element accepts a `%SERVERNAME%` string that is replaced with the name of the server when the log is created. The default log file location is `${server.output.dir}/logs/zosConnect`. For more information on the available configuration attributes and default values see the documentation for z/OS Connect 1.0 and z/OS Connect 1.2.

You can also configure the `fileSystemLoggerInterceptor` element for specific services.

```
<fileSystemLoggerInterceptor id="serviceYFileSystemLogger"  
    logName="service1Log"  
    logPath="/zosConnect/logs"  
    logOption="RESPONSE"  
    maxPayloadSize="30720"/>  
<zOsConnectInterceptors id="serviceYInterceptorList" interceptorRef="serviceYFileSystemLogger" />  
<zOsConnectService serviceName="serviceY" serviceRef="serviceY" interceptorsRef="serviceYInterceptorList"/>  
<usr_myService id="serviceY"/>
```

In the example, all z/OS Connect service requests are logged in a file that is called `service1Log_yyyy-MM-dd_HH_mm_ss_SSS.log` and in the `/zosConnect/logs` path. The log path is a fully qualified path. Only response data is logged for all incoming requests that target the `serviceY` service. Because the maximum JSON payload is configured to be 30,720 characters, any JSON (response) payload that is greater than 30,720 characters is truncated to the configured maximum payload size.

2. (Optional) Configure the `bufferedLogging` and the `bufferSize` attribute definitions to enable buffered logging. The default buffer size is 8 kilobytes. All records in the buffer are flushed to the disk when the buffer becomes full. Using buffered logging is appropriate when performance is a concern and when loss of unflushed records during a failure condition is acceptable.

```
<fileSystemLoggerInterceptor id="globalFileSystemLogger"  
    logName="globalLog_%SERVERNAME%"  
    bufferedLogging="true"  
    bufferSize="16384"/>
```

3. (Optional) Configure the `rolloffLogPolicy` attribute. This policy states that when the active log file reaches the specified or default file size of 50 megabytes, a new file is created. A new file can also be created when the specified or default time of 24 hours expires since the active log file was created. In the following example, a file is created when the file reaches 16 kilobytes in size. The naming schema is the same: `globalLog_myServer1_yyyy-MM-dd_HH_mm_ss_SSS.log`. The difference between the names of the created log files is the time stamp that is used when a given file is created:

```
<fileSystemLoggerInterceptor id="globalFileSystemLogger"  
    logName="globalLog_%SERVERNAME%"  
    rolloffLogPolicy="SIZE"  
    rolloffLogPolicySize="16384"/>
```

## Defining z/OS Connect message payload transformations



8.5.5.2

IBM® z/OS® Connect provides the ability to optionally transform request and response payloads that are used for calling a business asset on z/OS operating systems. You can create message payload

transformers can be created to satisfy specific needs by implementing the `com.ibm.wsspi.zos.connect.DataXform` Service Provider Interface (SPI), which is included with z/OS Connect.

## About this task

z/OS Connect provides an implementation that requires the request and response message format be JSON. This feature supports the conversion of the request to a byte array, which can be mapped by a native language Cobol, PL/I, or C structure. This language structure of the target program, or copy book, which includes a description of the **in** and **out** parameters, is used to generate a binding file, and JSON request and response schema files by using a z/OS Connect-provided utility. The binding file that is generated by this utility is used by z/OS Connect to complete the data conversion to and from JSON and native data formats as requests arrive and responses are returned. You can retrieve the JSON schemas for the request and response message with a REST API call that is provided by z/OS Connect.

z/OS Connect provides the `zosConnectService` configuration element that enables the administrator to configure a set of attributes that apply to a particular service. One of these attributes is `dataXformRef`, which points to a data transformation configuration that is to be used for a specific service. This task describes how to request that the z/OS Connect-supplied data transformer be used.

## Procedure

1. Update the `zosConnectService` element for each service in your `server.xml` configuration for which you want to enable the z/OS Connect-supplied data transformation.

```
<!-- z/OS Connect service definition -->
<zosConnectService id="zcs1"
  serviceName="recordOpsCreate"
  serviceRef="wola0psCreateService"
  dataXformRef="xformJSON2btye"/>
```

2. Create the associated `zosConnectDataXform` element.

```
<!-- z/OS Connect data transformation provider -->
<zosConnectDataXform id="xformJSON2Byte"
  bindFileLoc="/u/bindfiles" bindFileSuffix=".bnd"
  requestSchemaLoc="/u/json" responseSchemaLoc="/u/json"
  requestSchemaSuffix=".json" responseSchemaSuffix=".json"/>
```

For more information about the configurable attribute definitions associated with the `zosConnectDataXform` element, see the documentation for the “z/OS Connect” on page 959 feature.

3. Optional: Configure a data transformer that applies to all services. Set the `globalDataXformRef` of the `<zosConnectManager>` element to the configured data transformer's ID that is intended for global use. If both global and service data transformers are defined and requests come in for a service with a configured data transformer, z/OS Connect will use the data transformer configured specifically for the service.

```
<zosConnectManager id="zosConnectGlobals" globalDataXformRef="globalDataXform"/>
```

```
<!-- z/OS Connect data transformation provider -->
<zosConnectDataXform id="globalDataXform"
  bindFileLoc="/u/bindfiles" bindFileSuffix=".bnd"
  requestSchemaLoc="/u/json" responseSchemaLoc="/u/json"
  requestSchemaSuffix=".json" responseSchemaSuffix=".json"/>
```

4. 8.5.5.8 Optional: Configure settings such as `pollingRate` and `updateTrigger` to fine tune the monitoring actions. By default, the directories associated with a data transformation definition are monitored for new files and file updates. For more information about these configuration attributes see the `zosConnectDataXform` element section under `zosConnect-1.0` and `zosConnect 1.2`.

```
<zosConnectDataXform id="ibmDataXform2"
  bindFileLoc="/zosConnect/banking/bind/" bindFileSuffix=".bnd"
  requestSchemaLoc="/zosConnect/banking/reqSchema" requestSchemaSuffix=".json"
  responseSchemaLoc="/zosConnect/banking/respSchema" responseSchemaSuffix=".json" pollingRate="500ms">
</zosConnectDataXform>
```

In the example, directories /zosConnect/banking/bind,/zosConnect/banking/reqSchema, and /zosConnect/banking/respSchema are polled for file updates every 500 milliseconds. If the pollingRate and updateTrigger configuration attributes are not configured, the default values of polled and 2 seconds are used, respectively. If you do not need file monitoring, you can disable it by setting the updateTrigger attribute to disabled. If you prefer to trigger a manual refresh of certain files, set the updateTrigger attribute to mbean and use file notification mbean:

com.ibm.ws.kernel.filemonitor.FileNotificationMBean to trigger the updates; for example:

```
String[] MBEAN_METHOD_SIGNATURE = new String[] {Collection.class.getName(),Collection.class.getName(),Collection.class.getName()};
JMXConnector jmxConnector = ...;
MBeanServerConnection mbsc = jmxConnector.getMBeanServerConnection();
ObjectName fileMonitorMBeanName = new ObjectName("WebSphere:service=com.ibm.ws.kernel.filemonitor.FileNotificationMBean");
```

```
List<String> paths = new ArrayList<String>();
paths.add("/zosConnect/banking/bind/customer.bnd");
paths.add("/zosConnect/banking/reqSchema/customer_request.json");
paths.add("/zosConnect/banking/respSchema/customer_response.json");
```

```
Object[] params = new Object[] { null, paths, null };
mbsc.invoke(fileMonitorMBeanName, "notifyFileChanges", params, MBEAN_METHOD_SIGNATURE);
```

The example uses the restConnector-1.0 feature to trigger the update of files customer.bnd, customer\_request.json, and customer\_response.json. For more information about how to create a secure JMX connection see the documentation on “Configuring secure JMX connection to Liberty” on page 1642

## Creating binding and schema files for use with z/OS Connect



0.5.5.2

z/OS Connect provides the ability to optionally transform request and response payloads that are used for calling a business asset on z/OS operating systems. z/OS Connect supplies two new utilities called BBGLS2JS and BBGJS2LS.

### Before you begin

Before you create your binding and schema files, make sure that your setup complies with these preconditions:

- Your high-level language data structures must meet the following criteria:
  - The data structures must be defined separately from the source program; for example, in a COBOL copybook.
  - If your PL/I or COBOL application program uses different data structures for input and output, the data structures must be defined in two different members in a partitioned data set. If the same structure is used for input and output, the structure must be defined in a single member.
  - For C and C++, your data structures can be in the same member in a partitioned data set.
- The language structures must be available in a partitioned data set.
- You must define to Open Multiple Virtual Storage (OMVS) the user ID that BBGLS2JS or BBGJS2LS uses to run.
- The user ID must have read permission to z/OS® UNIX and PDS libraries, and write permission to the directories that are specified on the LOGFILE, WSBIND, and JSON-SCHEMA-REQUEST and JSON-SCHEMA-RESPONSE output parameters.
- The user ID must have a sufficiently large storage allocation to run Java™. You can use any supported version of Java. The BBGLS2JS/BBGJS2LS utilities use the Java version that is specified by JAVA\_HOME in the USS environment by default. Otherwise, the ID uses the Java version specified on the PATH statement.

## About this task

The BBGLS2JS utility reads a COBOL copybook or PLI, or C structure file and generates a binding file and JSON schema files. The BBGJS2LS utility reads a JSON schema and generates the corresponding binding file and language structure file (COBOL copybook or PL/I, or C structure header file). The utilities are similar to the existing DFHLS2JS and DFHJS2LS tools, which are part of the CICS Transaction Server Mobile Extensions feature pack. While the input parameters are the same, the symbolic parameters are different.

## Procedure

1. Obtain the BBGLS2JS JCL procedure. The BBGLS2JS and BBGJS2LS JCL procedures are available on GitHub. For information about how to use the JCL, see the readme file on GitHub. You will need to copy the JCL procedure from this location into a member named BBGLS2JS in a JCL procedure library on your z/OS system.
2. Use the BBGLS2JS procedure to generate a z/OS Connect service binding file from a language structure. You will need to provide JCL to invoke the BBGLS2JS procedure with the input parameters. Refer to the BBGLS2JS reference documentation for information on the input parameters and an example job to help you use the procedure. When you submit the BBGLS2JS procedure, the utility generates the service binding file to the location that you specified with the WSBIND parameter. The generated JSON schemas are placed in the location that you specified with the JSON-SCHEMA-REQUEST and JSON-SCHEMA-RESPONSE parameters.
3. Review the generated JSON schema. These schemas are used to define the input and output data formats for interacting with the z/OS Connect service. The application developer must use these schemas when creating an application to call the service and pass the JSON request payload.

**Note:** Changing the generated schema invalidates the generated binding file at WSBIND. If you want to change the schema, for example, to rename the fields within the schema, you must use BBGJS2LS to generate a new binding file, and a new set of language structures. The application program must be re-compiled to use the new language structures.

## Auditing and tracking with z/OS Connect



Audit and track requests with z/OS<sup>®</sup> Connect, which includes an interceptor that records data to the z/OS SMF data store.

## About this task

You can enable the interceptor in z/OS Connect on a single or group of z/OS Connect services. The z/OS Connect audit interceptor records request activity to the SMF data store on z/OS operating systems. SMF type 120, subtype 11 records are generated.

The SMF data in the 120-11 record contains the standard header for SMF records. Then, there are two triplets. The first triplet points to the server identification section of which there is one instance. The second triplet points to the user data section of which there can be multiple instances.

**The server data section consists of the following parameters: (values in decimal)**

- Offset Length Data
- 0 4 Version (1)
- 4 8 System name
- 12 8 Sysplex name
- 20 8 Job id(jsabjbid)
- 28 8 Job name (jsabjbnm)

- 36 8 SToken (assbstkn)

**The user data consists of the following parameters (values in decimal):**

- Offset Length Data
- 0 4 Version (1)
- 4 4 Type
- 8 4 Length of data (user data sections are 2 K, this field indicates how much of that is used)
- 12 ? Data

**The user data consists of the following parameters (values in decimal):**

For z/OS Connect the user data type is 102 (decimal). The data contains the following parameters:

- Offset length Data
- 0 4 Version (3)
- 4 8 Arrival time (STCK format)
- 12 8 Completion time (STCK format)
- 20 64 Target URI (EBCDIC, right-padded with blanks)
- 84 4 Input payload length in bytes
- 88 64 Service name (EBCDIC, right-padded with blanks)
- 152 8 Method (EBCDIC)
- 160 4 Respond length in bytes
- 164 64 User name (EBCDIC, right-padded with blanks)
- 228 23 Request id (bytes, right-padded with zeros)
- 251 1 Boundary padding (zero)
- 252 64 Service grouping name (EBCDIC, right-padded with blanks)
- 316 8 Mapped user name (EBCDIC, right-padded with blanks) Only valid on version 3 or later.

## Procedure

1. Enable the z/OS Connect-provided audit interceptor for a service or set of services. The z/OS Connect-supplied audit interceptor implements the `com.ibm.wsspi.zos.connect.Interceptor` SPI to store auditing/tracking information in the z/OS System Management Facility (SMF) data sets. The following is an example that shows how to enable the audit interceptor for a single service:

```
<!-- Audit interceptor configuration -->
<auditInterceptor id="auditInterceptor" sequence="1"/>

<!-- Interceptor list configuration -->
<zosConnectInterceptors id="interceptorList1" interceptorRef="auditInterceptor"/>

<!-- z/OS Connect service definitions -->
<zosConnectService id="zcs1" serviceName="recordOpsCreate" serviceRef="wola0psCreateService"
  interceptorsRef="interceptorList1"/>
```

2. Retrieve live statistic data. Feature start time, total number of service requests and the distribution of requests are available by using this operational capability. Valid authenticated clients are able to use a HTTP GET for one of the following URLs to retrieve statistics about the z/OS Connect server:
  - Get statistics for a single service:
 

```
https://<hostname:port>/zosConnect/services/HelloWorld?action=getStatistics
```
  - Get statistics for all services in the server:
 

```
https://<hostname:port>/zosConnect/operations/getStatistics
```
  - Get statistics for all services under a single service provider by specifying the `provider=<service provider name>` query parameter. For example to retrieve statistics for all services associated with the provider name of **WOLA-1.0** use the following URL:

https://<hostname:port>/zosConnect/operations/getStatistics?provider=WOLA-1.0"

- The response data is returned in JSON object format.

## z/OS Connect high availability



8.5.5.2

The z/OS® Connect file contains the list of service definitions, interceptors, and data transformation configuration that you can use for high availability and failover. You can include the z/OS Connect file in your `server.xml` file, and share the configuration across multiple servers that run on the same LPAR or span multiple z/OS logical partitions (LPARs). The z/OS Connect `action=start`, `stop`, and `status` operations are not supported for WOLA-based services when you share the `server.xml` file between servers.

Additionally, the IBM HTTP Server Apache web server with the WebSphere Application Server plug-in can be placed in front of these servers to spread requests across them. You might also include Sysplex Distributor, or Distributed Virtual IP (DVIPA) in your topologies and z/OS Connect.

## Configuring security for z/OS Connect



8.5.5.2

The z/OS connect application can be accessed by authenticated users that are also authorized under the `zosConnectAccess` role. You can configure group authorization at the service definition level. Group authorization is supported for SAF and LDAP group types.

### About this task

Users must be authenticated before the z/OS Connect application can be accessed.

The default authentication mechanism required by z/OS Connect is `CLIENT_CERT`. Users must be authorized under the `zosConnectAccess` role to be able to access the z/OS Connect application. The required transport mechanism is HTTPS.

8.5.5.7

You can configure z/OS Connect to run without any security constraints by setting the `requireSecure` and `requireAuth` attribute definitions. These attributes are defined under the `zosConnectManager` element, which applies to all configured services, or it is defined under the `zosConnectService` element for a specific service. If the attributes are defined under both the `zosConnectService` element and globally under the `zosConnectManager` element, the value defined under `zosConnectService` is used. See `zosConnectManager` and `zosConnectService` for more information on those attributes.

In order to provide a finer level of security, z/OS Connect offers the ability to constrain access based on group authorization that can be configured through SAF or LDAP. For this, z/OS Connect defines three levels of authority:

- Administrator - IUsers with administrator authority have the authority to query services, perform operational tasks on them, and invoke them.
- Operations - Users with operations authority are able to perform tasks on services such as stop, start, etc. but they do not have authority to invoke services.
- Invoke - Users with invoke authority are able to invoke services, but have no other authority.

z/OS Connect supplies an authorization interceptor that implements the `com.ibm.wsspi.zos.connect.Interceptor()` SPI. This interceptor supports both SAF and LDAP. This

interceptor uses the `getGroupsForUser()` security API internally to determine which groups the current user is in, and then compares these groups to the groups provided on the service definition or in the global definition.

When the z/OS Connect supplied authorization interceptor is enabled, the RACF or LDAP group names that are associated with users can also be associated with any of the groups that are mentioned previously at the global or service definition levels. At the global level, they can be defined under the `<zosConnectManager>` configuration element. The attributes that are defined at this level include: `globalAdminGroup`, `globalOperationsGroup`, and `globalInvokeGroup`. If configured, they apply to all configured services. If more granularity is wanted, the groups can also be configured at the service level under the `<zosConnectService>` configuration element. The attributes that are defined at that level are: `adminGroup`, `operationsGroup`, and `invokeGroup`. These values, if specified, override the values that are defined globally.

When an authorization interceptor is defined at the global level, authorization checks are done one time for all services. When you use `/zosConnect/operations/getStatistics` request for more than one service and service discovery, then the user gets information on all services that are registered with z/OS Connect when the following conditions exist:

- The user passes the authorization check
- No other conditions prevent service information from being returned

If the authorization interceptor is placed in a service level definition, access to information for those services are limited to users that are in that service definition.

For example, given the following configuration with the authorization interceptor defined at the service level:

User "USR1" Groups: ADMINS1, ADMINS2

User "USR2" Groups: OPERATS1

User "USR3" Groups: ADMINS2, OPERATS1

z/OS Connect configuration:

```
<!-- z/OS Connect global configuration. It applies to all services. -->
<zosConnectManager globalAdminGroup="ADMINS1" globalOperationsGroup="OPERATS1" globalInvokeGroup="INVOKES1"/>

<!-- Interceptor configuration -->
<zosConnectInterceptors id="interceptorList1" interceptorRef="zosConnectAuthorizationInterceptor"/>
<authorizationInterceptor id="zosConnectAuthorizationInterceptor"/>

<!--Service 1-->
<zosConnectService serviceName="service1" serviceRef="service1Ref" adminGroup="ADMINS2" operationsGroup="OPERATS2" int

<!--Service 2-->
<zosConnectService serviceName="service2" serviceRef="service2Ref" operationsGroup="OPERATS2" interceptorsRef="intercep

<!--Service 3-->
<zosConnectService serviceName="service3" serviceRef="service3Ref" adminGroup="ADMINS1" interceptorsRef="interceptorLis
```

Table 114. . User data access

	service1	service2	service3
USR1	X	X	X
USR2	--	--	X
USR3	X	--	X

## Procedure

1. Setup user authentication to access the z/OS Connect application. To setup client certificate authentication, see the documentation on configuring your web application and server for client certificate authentication. To setup authentication through a registry, see the documentation on authenticating users in Liberty.

Sample 1: Basic registry configuration using steps outlined in the documentation for configuring a basic user registry for Liberty.

Server.xml:

```
<featureManager>
  <feature>zosConnect-1.0</feature>
  <feature>ssl-1.0</feature>
  <feature>appSecurity-2.0</feature>
</featureManager>
```

```
<!-- Define a keystore. -->
<keyStore id="defaultKeyStore" password="Liberty"/>
```

```
<!-- Fail over to basic authentication -->
<webAppSecurity allowFailOverToBasicAuth="true"/>
```

```
<!-- Basic registry definition -->
<basicRegistry id="basic1" realm="zosConnect">
  <user name="Fred" password="fredpwd"/>
</basicRegistry>
```

Sample 2: SAF registry configuration using steps outlined in the documentation for activating and configuring the SAF registry on z/OS.

Server.xml:

```
<featureManager>
  <feature>zosConnect-1.0</feature>
  <feature>ssl-1.0</feature>
  <feature>appSecurity-2.0</feature>
  <feature>zosSecurity-1.0</feature>
</featureManager>
```

```
<!-- Saf registry definition -->
<safRegistry id="saf" realm="zosConnect"/>
```

RACF setup. For more details follow the documentation on Liberty: Accessing z/OS security resources using WZSSAD:

```
# Define the APPL class based on the default security prefix called BBGZDFLT.
RDEFINE APPL BBGZDFLT UACC(NONE)
```

```
# Activate the APPL class.
SETROPTS CLASSACT(APPL)
```

```
# For FRED to be authenticated by the server, assign FRED READ access to the APPLID in the APPL class.
PERMIT BBGZDFLT ID(FRED) ACCESS(READ) CLASS(APPL)
```

```
# The unauthenticated user ID (i.e. WSGUEST by default) requires READ access to the APPLID in the APPL class
PERMIT BBGZDFLT CLASS(APPL) ACCESS(READ) ID(unauthenticatedUserId)
```

```
# Grant the server permission to make authentication calls.
RDEFINE SERVER BBG.SECPFY.BBGZDFLT UACC(NONE)
PERMIT BBG.SECPFY.BBGZDFLT ID(serverId) ACCESS(READ) CLASS(SERVER)
```

Note that the server needs to be granted permission to use the SAFCREDAUTH authorized service routines. See the documentation on enabling z/OS authorized services on Liberty for z/OS for more details.

2. Setup user authorization to access the z/OS Connect application by assigning users the `zosConnectAccess` role. To do so, see the documentation on configuring authorization for applications on Liberty.

Add the following to the `server.xml` file configuration outlined in step 1 of sample1:

```
<authorization-roles id="zos.connect.access.roles">
  <security-role name="zosConnectAccess">
    <user name="Fred"/>
  </security-role>
</authorization-roles>
```

Sample2: Authorization configuration using SAF/RACF:

- a. Add the following to the configuration outlined in step 1 of sample2.

```
<safAuthorization id="saf2" />
```

- b. RACF setup. Commands to assigning FRED the `zosConnectAccess` role:

```
RDEFINE EJBROLE BBGZDFLT.zos.connect.access.roles.zosConnectAccess
UACC(NONE)
PERMIT BBGZDFLT.zos.connect.access.roles.zosConnectAccess
CLASS(EJBROLE) ID(FRED) ACCESS(READ)
```

3. (Optional) Define groups for authorization when using z/OS Connect's authorization interceptor.

Sample 1: RACF Group definition when using SAF:

```
ADDGROUP OPERATS1 OMVS(GID(xxx)) OWNER(yyyy)
```

```
# Add user FRED under the OPERATS1 group
```

```
ADDUSER FRED DFLTGRP(OPERATS1) OMVS(UID(xxx) HOME(/xxxx) PROGRAM(/bin/sh)) NAME('USER FRED') NOPASSWORD
ALTUSER FRED PASSWORD(xxxxxxxx) NOEXPIRED
```

```
# Connect user Fred to the OPERATS1 group
```

```
CONNECT FRED GROUP(OPERATS1)
```

Note that the "OPERATS1" group can then be used when defining authorization groups to be used by

z/OS Connect's authorization interceptor. For example: `<zosConnectManager globalOperationsGroup="OPERATS1"/>` or `<zosConnectService serviceRef="service1" operationsGroup="OPERATS1"/>`

---

## Platform-as-a-service environment considerations for setting up Liberty

Platform-as-a-service (PaaS) environments, such as IBM Bluemix, Pivotal Cloud Foundry, and OpenShift Enterprise, provide management and monitoring of application instances, but they also have some restrictions. Because of the inherent characteristics of PaaS environments, some Liberty features are redundant or behave differently, and they are therefore not supported.

### Liberty server management restrictions

Features related to Liberty collectives do not apply to a PaaS environment because all Liberty server JVM instances are started, stopped, and managed by the PaaS infrastructure. The Liberty Admin Center feature is not designed to be used in a PaaS environment, where an application can be scaled to use multiple JVM instances without a collective controller. In this topology, a request to Admin Center could be directed to any of the running instances and have visibility only to the server on which the request runs.

The following administrative features are not supported in a PaaS environment:

- `adminCenter-1.0`
- `clusterMember-1.0`
- `collectiveController-1.0`
- `collectiveMember-1.0`

- dynamicRouting-1.0
- healthAnalyzer-1.0
- healthManager-1.0
- scalingController-1.0
- scalingMember-1.0

## File system restrictions

Most PaaS environments do not provide a persistent local file system to their applications. For Liberty, this impacts both the applications and the components within the server that write data locally and expect it to persist across a server JVM restart.

The Liberty transaction manager writes log files to the local file system when multiple resource managers are involved in the transaction. If the logs are not available after a JVM failure and restart, then transactions cannot be automatically completed and must be manually resolved to unlock data and to make it consistent across resource managers. To avoid this scenario, the Liberty buildpack or cartridge prevents transaction log records from being written and raises an exception to the application to prevent the second resource from enlisting. As a result, although you can still use transactions with a single XA resource, a second transactional resource cannot be enlisted in a transaction. Additionally, Web Services Atomic Transactions cannot be used because they always write log records.

If your PaaS environment provides persistent storage, then you can modify the Liberty buildpack or cartridge to enable two-phase transactions by removing the following Java property from the JVM configuration:

```
-Dcom.ibm.tx.jta.disable2PC=true
```

The following features depend on persistent local storage:

- wsAtomicTransaction-1.2
- Other features that use transactions, depending on the application behavior

## Network restrictions

In general, PaaS routers do not support Internet Inter-ORB Protocol (IIOP) traffic, so remote requests to Enterprise JavaBeans (EJB) components cannot be used. The following features depend on IIOP transport:

- appClientSupport-1.0
- appSecurityClient-1.0
- ejbRemote-3.2

In some situations, such as SSL termination at the router, Liberty relies on HTTP headers to describe aspects of the original client request. When you use SSL in a PaaS environment, the headers must be set by the PaaS router. On IBM Bluemix, these headers are already set, so you can use the `ssl-1.0` feature and any features that depend on it without changes. To get the expected behavior in other PaaS environments, you might need to configure the router to set these headers as described in NGINX and WebSphere Application Server.

The following features require the router to set HTTP headers:

- `ssl-1.0`
- Other features that depend on `ssl-1.0`, as listed in the *Features that enable this feature* section of “Secure Socket Layer” on page 951

---

## Chapter 6. Administering Liberty

A server configuration consists of a `server.xml` file, a `bootstrap.properties` file, and any optional files that are included by the two main configuration files. You can use WebSphere Application Server Developer Tools for Eclipse or a text editor to edit the configuration files. There is no administrative console for Liberty, but you can use Admin Center to administer Liberty servers and applications and other resources from a web browser on a smartphone, tablet, or computer.

### About this task

Liberty is configured by exception. The runtime environment operates from a set of built-in configuration default settings, and you only need to specify configuration that overrides those default settings. You do this by editing either the `server.xml` file or another XML file that is included in `server.xml` at run time.

Features are the units of functionality by which you control the pieces of the runtime environment that are loaded into a particular server. They are the primary mechanism that makes the server composable. The list of features that you specify in the server configuration provides a functional server.

When you first install and start the server, a feature manager and a default server configuration are available:

- By default, a server contains the `jsp-2.2` feature, to support servlet and JSP applications. You can use the feature manager to add the features that you need.
- Server configuration is by exception. When you specify the features that you need, the default configuration of those features provides a rich environment that is designed to cover most common requirements, therefore you only need to specify changes from the default configuration.

**8.5.5.0** You can organize Liberty servers into collectives to administer multiple Liberty servers at a time efficiently and accurately. For information about collectives, see “Setting up the server-management environment for Liberty by using collectives” on page 1134.

### Procedure

- 
- “Administering Liberty by using developer tools” on page 1556
- “Administering Liberty manually” on page 1564
- **8.5.5.0** Chapter 7, “Extending Liberty,” on page 1771

---

## XML escape characters

You need to escape specific XML characters in Liberty configuration files, such as the `server.xml` file because Liberty does not automatically escape these characters. If you use the Rational Application Developer tool, you do not need to manually escape these characters.

*Table 115. XML characters.* For more information, see Extensible Markup Language (XML) .

Original character	Escaped character
"	&quot;
'	&apos;
<	&lt;
>	&gt;

Table 115. XML characters (continued). For more information, see Extensible Markup Language (XML) .

Original character	Escaped character
&	&amp;

---

## Administering Liberty by using developer tools

### Distributed operating systems

You can modify how the workbench interacts with Liberty by using the server editor.

#### Procedure

1. In the Servers view, right-click the server and select **Open**.
2. The server editor opens.

#### What to do next

You can modify the publishing, timeout, and other settings regarding the interaction between the workbench and the server.

## Editing the Liberty configuration by using developer tools

### Distributed operating systems

You can modify the behavior of Liberty by editing the configuration. For example, you can configure which HTTP ports to use, what features are enabled, and logging and tracing settings.

#### Before you begin

For a description of the underlying process of configuring a server, and detailed information about specific aspects of server configuration, see “Administering Liberty manually” on page 1564.

#### About this task

The server configuration editor consists of two views: the Source view and the Design view. The Design view is a structured view of the file whereas the Source view is a text view. But both of them are views of the same server configuration file. The Design view has many features that help with the construction of some of the more complex elements in the server configuration such as data sources.

The following steps are demonstrated in the Design view.

#### Procedure

1. To open the Server Configuration editor, select any of the following options:
  - In the **Servers** view, right-click the server configuration and select **Open**.
  - In the **Enterprise Explorer** view, expand your server project and the server folder. Right-click the `server.xml` file and select **Open**.
2. Under the **Configuration Structure** section, the elements in the configuration are displayed.
3. Under the **Feature Manager** section, the details for the currently selected element are displayed. The details can also be modified here.
4. To add new elements, select **Server Configuration** under the **Configuration Structure** section then click **Add**.

5. To add child elements, select the parent element under the **Configuration Structure** section and then click **Add**.
6. You can remove or move elements by selecting the element and using the **Remove**, **Up**, and **Down** buttons.

## What to do next

You can use the key combinations from Table 116 in both the Source view and the Design view.

Table 116. Keyboard shortcuts

Key combination	Function
Ctrl+Space	Content assistance. It displays variables that have the correct type for the current field (int, string, and other code) or ids of the correct type for a reference field.
F3	Hyperlink to variable references and id references.

## Specifying the Liberty configuration with dropins files by using developer tools



8.5.5.6

You can specify the server configuration for Liberty by creating configuration dropins files and placing these files in the `configDropins` directory.

### About this task

You can use the dropins files to set a default configuration, or override configurations that are set in the `server.xml` file or included files. The server configuration validator includes configuration dropins files as part of the overall server configuration validation. The server configuration editor shows variables and references that are defined in dropins files in the appropriate content assistance and drop-down lists.

You can place configuration dropins files in either the `${server.config.dir}/configDropins/defaults` directory or in the `${server.config.dir}/configDropins/overrides` directory.

- If you place these files in the `defaults` directory, then the configuration is applied before the server configuration. In this case, the files provide default values, which you can override in the main `server.xml` file or the included files.
- If you place the configuration dropins files in the `overrides` directory, then the configuration is applied after the server configuration. In this case, the files override the main `server.xml` or included files.

For more information about configuration dropins files, see: “Using the configuration dropins folder to specify server configuration” on page 1593.

### Procedure

1. To create a configuration dropins file, right-click your server in the Servers view.
2. Complete one of the following options:
  - a. To create a configuration dropins file in the `defaults` directory, select **New > Configuration Dropins File > Defaults**
  - b. To create a configuration dropins file in the `overrides` directory, select **New > Configuration Dropins File > Overrides**.
3. Enter the name of the file that you want to create.
4. Click **OK**.

The new file is displayed.

5. To see the merged configuration, complete one of the following options:
  - a. Right-click the `server.xml` file in the Enterprise Explorer or Project Explorer view, and then select **Liberty > Open Merged View**.
  - b. In the Servers view, right-click on **Server Configuration** and select **Open Merged View**.The merged view of the server configuration shows the defaults at the beginning of the merged configuration. It also shows the overrides at the end of the merged configuration.

## Starting and stopping a server by using developer tools

You can start and stop a server by using the Liberty developer tools.

### Procedure

- To start a server:

In the Servers view, right-click the server and click **Start** to start the server or click **Debug** to start the server in the debug mode. Alternatively, click  to start the server, or click  to start the server in the debug mode.

**Tip:**  8.5.5.4 When you start a remote Liberty server, you can specify which debug port to use in the **Remote Start Settings** section of the server editor. The default port is 7777.

- To stop the server:

In the Servers view, right-click the server and click **Stop**. Alternatively, click  to stop the server.

**Tip:** In the Servers view, you must select the server entry to perform these tasks. Do not select the server configuration entry, for example Server Configuration [server.xml], to perform these tasks.

### What to do next

You can configure the server elements by using the tools.

## Switching a Liberty Docker server between run and debug mode by using developer tools

8.5.5.9

For your Liberty Docker server, you can use WebSphere Developer Tools to switch your server between run and debug mode. When you switch between these modes, the tools create a Docker image and a Docker container, which you can save.

### Before you begin

You must create a Liberty Docker server by using WebSphere Developer Tools. For more information about using WebSphere Developers Tools to create a Liberty server in a Docker container, see “Creating a workbench Liberty server in a Docker container by using developer tools” on page 1430.

### About this task

When you create a Liberty server in a Docker container, the run command and host mapped ports are fixed. As a result, when you switch a Liberty Docker server between run and debug modes, WebSphere Developer Tools commit a new Docker image based on your Docker container. This action preserves all of your changes to the container at that point. Then, the tools create a new container from the new image, but modify the run command to either run or debug the server. When you switch to debug mode, the tools map the debug port to the host.

The tools do not delete the original image and container. However, the tools remove any temporary images and containers when you switch modes. To avoid losing changes that you made to your server in debug mode, you can save the last temporary image and container when you delete a Liberty Docker server.

## Procedure

1. Switch your server from run mode to debug mode:
  - a. Open the Servers view in WebSphere Developer Tools by clicking **Window > Show view > Servers**.
  - b. Start your server in debug mode by right-clicking *your\_server* and selecting **Debug**.  
The tools go through the following steps:
    - 1) Disconnect from the *your\_server* container and stop the container.
    - 2) Commit the *your\_server* container to a new image that is named *your\_server\_debug\_websphere-liberty*
    - 3) Create a new container that is named *your\_server\_debug* from the *your\_server\_debug\_websphere-liberty* image.
    - 4) Connect to the *your\_server\_debug* container.
  - c. If the tools display the Server Execution Mode Switch window, click **OK** to continue.  
The tools display the Server Execution Mode Switch window only the first time that you switch the mode for your server.
2. Switch your server back to run mode from debug mode by right-clicking *your\_server* and selecting **Run**.  
The tools go through the following steps:
  - a. Disconnect from the *your\_server\_debug* container and stop the container.
  - b. Commit the *your\_server\_debug* container to a new image that is named *your\_server\_run\_websphere-liberty*
  - c. Create a new container that is named *your\_server\_run* from the *your\_server\_run\_websphere-liberty* image.
  - d. Connect to the *your\_server\_run* container.
3. Delete the *your\_server* server by right-clicking *your\_server* and selecting **Delete**.
4. Click **Yes** to save the *your\_server\_run* container and the *your\_server\_run\_websphere-liberty* image.

## Results

You switched your server from run mode to debug mode and back to run mode. When you switched back to run mode, you saved any changes that you made to the container and image when you were in debug mode.

## Defining a utility project as a shared library

### Distributed operating systems

You can define a utility project as a shared library and associate defined shared libraries with an application or web project.

### Before you begin

To use the shared library function in the workbench, you must create a utility project and define it as a shared library. The utility project is the only project type that can be used as a shared library.

## About this task

A shared library is an external Java archive (JAR) file that is used by one or more applications. Using shared libraries enables multiple application published on a server to use a single library, rather than use multiple copies of the same library. After you associate shared libraries with an application or project, the application or module class loader loads classes in the shared libraries and makes those classes available to the application or module.

## Procedure

To define a utility project as a shared library:

1. Create a utility project:
  - a. In the toolbar, select **File > New > Project**.
  - b. Expand **Java EE** and select **Utility Project**. Click **Next**.
  - c. In the **Project name** field, specify a name for the utility project.
  - d. Under the **Ear membership** section, clear the **Add project to an EAR** check box.
  - e. Under the **Target runtime** section, verify the WebSphere Application Server Liberty is selected.
  - f. Click **Finish**.
2. Define the artifacts in the newly created utility project. For example, you can add Java classes to the utility project.
3. Define the utility project as a shared library:
  - a. In the **Project Explorer** view, right-click the utility project and select **Properties > Liberty > Shared Library**.
  - b. In the **Shared library ID** field, type a string as an identifier for the shared library.
  - c. In the **Archive directory** field, type or browse to a directory where you want to place the compressed copy of your utility project as a JAR file. The file name convention of the JAR file is *utilityProjectName.jar*, where *utilityProjectName* is the name of the utility project.
  - d. In the **Liberty Shared Library** page, click **Apply** to confirm your changes. Click **OK** to close the Properties window.
4. Add the utility project to the server. **Distributed operating systems** For more details see “Adding and running an application on Liberty by using developer tools” on page 2141 topic.

## Results

Here is an example entry added to the server configuration (server.xml) file:

```
<library id="libid">
  <fileset dir="C:\temp" includes="Util.jar"/>
</library>
```

In addition, the JAR file is added in the specified archive directory. In the previous example, the `Util.jar` file is added in the `C:\temp` directory.

## Setting a web project to use shared libraries

### Distributed operating systems

If you have a utility project defined as a shared library, you can associate defined shared libraries with a web project.

## Before you begin

- **8.5.5.0** Define a utility project as a shared library.

## About this task

A shared library is an external Java archive (JAR) file that is used by one or more applications. Using shared libraries enables multiple application published on a server to use a single library, rather than use multiple copies of the same library. After you associate shared libraries with an application or project, the application or module class loader loads classes in the shared libraries and make those classes available to the application or module.

## Procedure

1. To set a web project to use shared libraries:
  - a. In the **Project Explorer** view, right-click your web project that you want to associate shared libraries.
  - b. Select **Properties > Liberty > Shared Libraries**.
  - c. When you click the **Add** button, a list of shared library **IDs** will appear. In the **IDs** field, specify one or more shared library identifiers that you want the project to reference. To specify multiple identifiers, use a comma-separated list. For example: ID1, ID2, ID3

**Tip:** The shared library identifier is the value specified in the **Shared Library ID** field from the Defining a utility project as a shared library task.

2. You might want to add its associating utility projects to the class path for compilation-purpose:
  - a. In the **Project Explorer** view, right-click your project that you are associating shared libraries.
  - b. Select **Properties > Java Build Path**.
  - c. Select the **Projects** tab.
  - d. Click **Add**.
  - e. Select the utility projects that the project references.
3. Develop the artifacts in the web project. For example, you can add a servlet in a web project that references classes in the shared libraries.
4. Add the web project to the server. **Distributed operating systems** For more details see “Adding and running an application on Liberty by using developer tools” on page 2141 topic.

## Results

Here is an example entry added to the server configuration (server.xml) file:

```
<application type="war" id="web" name="web" location="web.war">
  <classloader commonLibraryRef="libid"/>
</application>
```

## Exploring the runtime environment by using developer tools

### Distributed operating systems

You can use the **Runtime Explorer** view to browse the available servers. This view shows all of the available servers for the runtime environment as opposed to the **Servers** view, which shows only those servers that are configured in the workspace. In both the Runtime Explorer and Servers view, you can expand each server to show the configuration for that server.

## Before you begin

The application server that the Runtime Explorer view supports is the WebSphere Application Server Liberty.

## About this task

You can use the Runtime Explorer view to complete the following tasks:

- View the servers that are defined in a runtime environment.
- View the shared configurations files that are defined in a runtime environment.
- Create a server in a runtime environment.
-  **8.5.5.2** Create a runtime environment and optionally install add-ons from the Liberty Repository on the Downloads page on WASdev.net.
-  **8.5.5.6** Configure additional repositories.

## Procedure

To open the Runtime Explorer view:

1. In the toolbar of the workbench, select **Window > Show View > Other**.
2. In the **Show View** window, expand **Server** and select **Runtime Explorer**. Click **OK**.

## Displaying the server configuration in a merged view

### Distributed operating systems

You can use the **Merged Configuration** view to see a flattened view of the server configuration and any included configuration files.

## About this task

In the Server Configuration editor, under the **Configuration Structure** section, you can use the **Include** element to import files that contain additional configuration settings. The **Include** element can embed multiple layers of configuration files within the `server.xml` file, which can make the configuration difficult to read without tools. The **Merged Configuration** view provides a flattened view of the server configuration and any included configuration files. This is a read-only view and cannot be edited.

## Procedure

To display the server configuration in a merged view:

In the Servers view, right-click the server configuration and select **Open Merged View**.

## Example

Here is an example of the source code for the `server.xml` file. Look at the **include** tag which imports the `common.xml` file:

```
<server>
  <featureManager>
    <feature>jsp-2.2</feature>
    <feature>servlet-3.0</feature>
  </featureManager>
  <application id="Web2.5" location="Web2.5.war" name="Web2.5" type="war"/>
  <include location="common.xml"/>
</server>
```

Here is an example of the source code for the `common.xml` file:

```
<server>
  <application id="Setup" location="Setup.war" name="Setup" type="war"/>
</server>
```

Look under the **Configuration Structure** sections to see the difference between the Server Configuration editor and Merged Configuration view. The Merged Configuration view replaces the **Include: common.xml** element from the Server Configuration editor with **Application: Setup** element.

## Viewing the schema documentation for the server configuration

### Distributed operating systems

You can view the schema documentation for the server configuration (server.xml file) within the workbench. The documentation provides information about the configuration elements that are available, the default settings, and details for each of the elements.

### Procedure

In the **Servers** view, right-click on the server configuration and select **Open Schema Reference**.

## Generating a Liberty server dump using developer tools

Using the Liberty Utilities menu, you can generate a server dump for support.

### About this task

You can use the Utilities menu of your Liberty server to generate a server dump to capture all service-related information for support.

### Procedure

1. In the **Servers** view, right-click your Liberty server, and select **Utilities > Generate dump for Support...**
2. In the **Generate Dump** page, enter a location for the dump archive or use the **Browse** button. Then, click **Finish** to create the server dump file.
3. In the **Console** view, the path to the server dump is indicated:

```
Server TestServer dump complete in
D:\LibertyUnzip\wlp\usr\servers\TestServer\TestServer.dump-12.03.22_15.00.11.zip.
```

## Packaging a Liberty server by using developer tools

You can create a compressed file containing a server runtime environment, server configuration, and applications using the packaging wizard.

### About this task

Because a Liberty server is lightweight, you might find it useful to package up your applications and server in a compressed file. You can then store this package, distribute it to colleagues, use it to deploy the application to a different location or to another machine, or even embed it in your product distribution.

### Procedure

1. In the **Servers** view, stop the server.
2. Right-click your Liberty server, and select **Utilities > Package Server...**

3. In the Package Server page, in the **Archive** field, type a filename and path for your archive package, or click **Browse** to locate a filename and path. This filename can include a full path name. If the full path is omitted, a compressed file called *package\_file\_name.zip* is created in the `${server.output.dir}` directory.
4. In the **Include** field, select whether to include:
  - **Full runtime (all)**
  - **Minimal runtime (minify)**
  - **No runtime (usr)**

For details on these include options, see Packaging a Liberty server from the command prompt topic.

5. Click **Finish**.

## Adding a data source by using developer tools

You can add a data source to your application using the developer tools.

### Procedure

1. In the Project Explorer view, expand *liberty\_name* > **servers** > *server\_name* > **server.xml**, and select **Open**.
2. In the design view, select **Server Configuration**, and click **Add**.
3. On the Select item to add to Server Configuration: page, select **Data Source** and fill in the JNDI name.
4. On the Data Source Details panel, alongside **JDBC Driver**, click **Add**.
5. On the Configure a JDBC driver page,
  - In the **Library ref:** field, select an option from the drop-down list, or click **Add** to create a new one.
    - In the **Fileset ref:** field, select an option from the drop-down list, or click **Add** to create a new one.
      - In the **Base directory** field, type a path for your base directory or click **Browse** to locate a library location path. Use the drop-down arrow next to Browse to choose between browsing for a relative path or browsing for an absolute path.
      - In the **Includes** field, type the name of your data source, for example *derby.jar*, or click **Browse** to locate the data source archive file that you want to include.
      - In the **Excludes** field, type the archives that you want to exclude, or click **Browse** to locate the data source archive file that you want to exclude.
6. Your JDBC data source has been added to your application.

---

## Administering Liberty manually

You can administer Liberty from the command prompt, configure it with web server plug-ins, and capture its status. You can package a Liberty server configuration along with the applications that it runs, for distribution to colleagues, or installation on other systems. If available, you can use the Equinox OSGi console to aid with debugging.

### About this task

The *server.xml* file is the primary configuration file for the server. You can edit this file, and the files it includes, in a text editor. You can also change the location of the *server.xml* file. However, for most configurations you do not need to do this.

The *bootstrap.properties* file is used to specify properties that need to be available before the main configuration is processed. If you update the *bootstrap.properties* file, you must restart the server for the changes to take effect.

## Example

All the elements that can be configured in the `server.xml` file, and the files it includes, are described in “Liberty features” on page 826. However, the only required element is a server definition:

```
<server/>
```

Beyond this server definition, you only specify overrides and additions to the default configuration values. For example, to change the transaction timeout value, you specify:

```
<transactions timeout="30" />
```

Some attributes can have multiple values. For example, you use a list of values to define the features that are to be provided by the server:

```
<server>
  <featureManager>
    <feature>servlet-3.0</feature>
    <feature>localConnector-1.0</feature>
  </featureManager>
</server>
```

See also “Adding and removing Liberty features” on page 1587.

Where multiple instances of a resource type can be configured, for example applications or data sources, you need only provide the attributes that are unique for the resource. You can let the other attributes use the default values, or override them as needed. Therefore the contents of the `server.xml` file can be brief. For example, here is a complete server configuration to run a web application:

```
<server>
  <featureManager>
    <feature>servlet_3.0</feature>
  </featureManager>
  <application name="snoop" location="/mywebapps/snoop" id="snoop" type="war"/>
</server>
```

For detailed information about specific aspects of server configuration, see the subtopics.

## Customizing the Liberty environment

You can customize the Liberty environment by using certain specific variables to support the placement of product binary files and shared resources in read-only file systems.

### About this task

The Liberty specific environment variables in the following list can be configured in the `server.env` file to customize the Liberty environment. The `${wlp.install.dir}` configuration variable has an inferred location that is always set to the parent of the directory that contains the launch script.

- `WLP_USER_DIR`

This environment variable can be used to specify an alternative location for `${wlp.user.dir}`. This variable must be an absolute path. If this variable is specified, the runtime environment looks for shared resources and server definitions in the specified directory. The `${server.config.dir}` is equivalent to `${wlp.user.dir}/servers/serverName`. If this environment variable is not specified, `${wlp.user.dir}` is set to `${wlp.install.dir}/usr`.

- `WLP_OUTPUT_DIR`

This environment variable can be used to specify an alternative location for server generated output such as logs, the workarea directory, and generated files. Files in the logs directory can include `console.log`, `messages.log`, and any generated FFDC files. Generated files can include server dumps that are created with the `server dump` or `server javadump` command. This variable must be an absolute

path. If this environment variable is specified, `${server.output.dir}` is set to the equivalent of `WLP_OUTPUT_DIR/serverName`. If this environment variable is not specified, `${server.output.dir}` is the same as `${server.config.dir}`.

When the server command is used, the server process uses the output directory as its current working directory.

- **z/OS** WLP\_ZOS\_PROCEDURE

This environment variable can be used to specify the name of an STC procedure to be used to start the server as a z/OS started task rather than as a USS background process. By default, the command port remains enabled to allow continued administration of the server from the server script. Optionally, the command port can be manually disabled restricting server administration to just the z/OS operator console, see *Specifying Liberty bootstrap properties*.

- **8.5.5.0** WLP\_DEBUG\_ADDRESS

This environment variable can be used to specify an alternative port when you run the server in debug mode. The default value is 7777. When Liberty is run in debug mode from the server command, the following values are set `JAVA_DEBUG="-Dwas.debug.mode=true -Dcom.ibm.websphere.ras.inject.at.transform=true -agentlib:jdwp=transport=dt_socket,server=y,suspend=y,address=${WLP_DEBUG_ADDRESS}"`. However, if you run Liberty from the **ws-server.jar** executable JAR file, or the embedded Liberty server SPI, then you must use the same settings to enable debug mode for Liberty.

You can specify `WLP_OUTPUT_DIR`, `WLP_USER_DIR`, and **8.5.5.0** `WLP_DEBUG_ADDRESS` environment variables in `server.env` files. You can also specify JVM options in `jvm.options` files. Both `server.env` and `jvm.options` files work only when you use the server management script. If you use the **ws-server.jar** executable JAR file to launch your server, these files are not supported.

## Procedure

- Specify environment variables by using `server.env` files.

You can use `server.env` files at the installation and server levels to specify environment variables such as `JAVA_HOME`, `WLP_USER_DIR`, and `WLP_OUTPUT_DIR`. For example:

```
# Use a specific Java binary
JAVA_HOME=/opt/ibm/java-i386-60/jre
# JAVA_HOME=c:\Java
```

### Note:

- The `server.env` files support only key=value pairs.
- Empty lines and lines that start with the # character are ignored.
- There are no escape characters; all characters are literal, including backslashes and leading and trailing white space.
- There should be no white space surrounding the equals "=" sign.
- Shell and variable expansion are not supported.
- `WLP_USER_DIR` can be specified only in the `${wlp.install.dir}/etc/server.env` file because the purpose of this variable is to specify where the remaining configuration is located. After the remaining configuration is found and merged, no further configuration in a different location is expected, or supported.

The server management script searches for `server.env` files in two locations: `${wlp.install.dir}/etc/server.env` and `${server.config.dir}/server.env`. If both files are present, the contents of the two files are merged; values in the server-level file take precedence over values in the runtime-level file.

You can also specify these environment variables in the shell environment, but the `server.env` files take precedence over those variables.

- Customize JVM options by using `jvm.options` files.

You can use `jvm.options` files at the runtime and server levels to specify more server startup options, for example, `-X` arguments. The options are applied when the start, run, and debug actions are started through the server management script. Be sure to specify only one option per line. For example:

```
# Set the maximum heap size to 1024m.
-Xmx1024m

# Set a system property.
-Dcom.ibm.example.system.property=ExampleValue

# Enable verbose output for class loading.
-verbose:class

# Enable verbose garbage collection.
-verbose:gc

# Specify an alternate verbose garbage collection log on IBM Java Virtual Machines only.
-Xverbosegclog:verbosegc.log

# Specify additional verbose garbage collection options on HotSpot Java Virtual Machines only.
-Xloggc:verbosegc.log
-XX:+PrintGCDetails
-XX:+PrintGCTimeStamps
-XX:+PrintHeapAtGC
```

The server management script searches for `jvm.options` in two locations: `${wlp.install.dir}/etc/jvm.options` and `${server.config.dir}/jvm.options`. If both files are present, the options in the `${server.config.dir}/jvm.options` file are used.

**Note:**

- Do not put property values in quotes.
- Empty lines and lines that start with the `#` character are ignored.
- There are no escape characters; all characters are literal, including back-slashes and leading and trailing white space.
- There should be no white space surrounding the equals `=` sign.
- Shell and variable expansion are not supported.

## What to do next

If you start the Liberty server by using the server script, all of the operating system environment variables from the current session are available. If you start the server by using either the MBean or the Admin Center, the only available environment variables are those variables that are available to a remote command that is running on that system.

## Administering Liberty from the command line

You can use the server command and `ws-server.jar` executable JAR file to create a server, to start, or stop a server, to check if it is running, or debug a server.

### About this task

The `wlp/bin` directory contains a script called `server` to help with controlling the server process. The syntax of this script is as follows:

```
server <action> [server] [options]
```

For available values of the **options**, see “Liberty:server command options” on page 1569.

**Avoid trouble:** The administrative console allows a start and a stop of a Liberty server that is a cluster member of an auto-scalable cluster, but only when the server is in maintenance mode. Starting or

stopping a Liberty server from the command line when the Liberty server is a cluster member of an auto-scalable cluster can lead to unpredictable results.

This script supports the following actions:

**create** A command that creates a new server.

**run** A command that launches the server in the foreground.

**debug** A command that runs the named server in the console foreground after a debugger connects to the debug port. The default port is 7777. **0.5.5.0** You can use the `WLP_DEBUG_ADDRESS` variable to specify an alternative port.

**dump** A command that creates a snapshot of a server and saves the result into an archive file for further tuning and diagnosis.

### **0.5.0.1** **javadump**

A command that creates a snapshot of the server Java virtual machine (JVM) and saves the result into files. Each dump type creates a file, but not all dump types are supported by all virtual machines. The default directory for dump files is `${server.output.dir}`. To set a different default directory, you must use an IBM JVM and set the following environment variables:

- **IBM\_HEAPDUMPDIR**
- **IBM\_COREDIR**
- **IBM\_JAVACOREDIR**

### **package**

A command that packages a server.

**start** A command that launches the server as a background process.

**z/OS** You can use the `WLP_ZOS_PROCEDURE` environment variable to specify the name of an STC procedure to be used to start the server as a z/OS started task rather than as a USS background process, see Customizing the Liberty environment.

**stop** A command that stops a running server.

**status** A command that checks to see whether a specified server is running.

### **version**

A command that displays the version information of current server and Java runtime environment.

**help** A command that gets command-line script help, including details of additional options.

**Note:** If a server is not specified on the command line, the action is performed against the default server instance, `defaultServer`, if it exists.

You can also carry out similar actions by using the executable JAR file `ws-server.jar` that is in the `${wlp.install.dir}/bin/tools` directory.

## **Example**

To run the server script on Windows systems:

```
server.bat create server_name
server.bat package server_name
server.bat run server_name
server.bat help server_name
```

To run the server script on other systems:

```
server create server_name
server package server_name
server run server_name
server help server_name
```

To run the executable JAR file `ws-server.jar` without using the `server` script:

```
java -javaagent:bin/tools/ws-javaagent.jar -jar bin/tools/ws-server.jar server_name --create
java -javaagent:bin/tools/ws-javaagent.jar -jar bin/tools/ws-server.jar server_name
java -javaagent:bin/tools/ws-javaagent.jar -jar bin/tools/ws-server.jar --help
```

The `--help` option provides information about additional command-line parameters for the executable JAR file `ws-server.jar`, such as `--stop`, `--version`, `--clean`, `--include`.

## Liberty:server command options

The **server** command supports starting, stopping, creating, packaging, and dumping a Liberty server. This topic describes all available options and exit codes that you can use with the **server** command and the equivalent executable jar file `ws-server.jar`.

### Syntax

The command syntax is as follows:  
`server action serverName [options]`

where the value of **action** represents the operation that you can perform on a Liberty server. See available administration operations for Liberty from the command prompt.

**Note:** If a server is not specified on the command line, the action is performed against the default server instance, `defaultServer`, if it exists.

### Options

The following options are available for the **server** command:

**--archive**="*path\_to\_the\_target\_archive\_file*"

Specifies a target file for the *package* **8.5.0.1** or *dump* operation. This path can be either a relative path, which is relative to the installation root directory of Liberty, or an absolute path. The default archive target is a compressed file with the server name, which is stored in the installation root directory. Use quotation marks if the value contains spaces. You can use this option for both *package* and *dump* operations.

**Distributed operating systems** **IBM i** **8.5.5.0** If you specify a `.jar` extension for your archive file name, the **server** command creates a new self-extracting archive file from which the Liberty server can be installed by using the **java** command; for more information, see "Installing Liberty by extracting a Java archive file" on page 1374. The `.jar` extension facility is not available on the z/OS platform.

**--clean**

Cleans all persistent cached information that is related to the specified server instance, which includes OSGi resolver metadata and persistent OSGi bundle data. If you use this option, the server will be required to recompute any cached data at the next startup, which might take more time than a restart that can reuse cached data.

**Note:** This option is not necessary for normal operation. IBM service might request that you use this option when you provide an interim fix, or if there is a suspected problem with the cached

data. **8.5.5.0** This option might also be necessary if you are developing a product extension, and you are either updating OSGi manifests or planning to clear persistent OSGi bundle data.

**--include=package\_option**

Specifies the files that you want to package, where *package\_option* can take one of the following values:

- `all` specifies to package all the files in the Liberty installation directory. If the `${WLP_USER_DIR}` and `${WLP_OUTPUT_DIR}` are defined in the `server.env` file, the files under them are packaged. This value applies only to the *package* operation.
- `usr` specifies to package the files in the `${WLP_USER_DIR}` directory. This value applies only to the *package* operation.
- **8.5.5.0** `minify` specifies to package only those parts of the runtime environment, and files in the `${WLP_USER_DIR}` directory, that are required to run the server, which minimizes the size of the resulting archive. This value applies only to the *package* operation.

**--include=diagnose\_option,diagnose\_option,...**

Specifies the type of diagnostic information to be captured. The value of **--include** is a comma-delimited list, which can contain any of the following values:

- `heap` is used to help diagnose the excessive memory consumption and memory leaks, which shows live objects in the memory and references between them. On IBM J9 virtual machines, the resulting file is named `heapdump.date.time.processID.sequenceNumber.phd`. On HotSpot virtual machines, the resulting file is named `java.date.time.processID.sequenceNumber.hprof`. This value applies to both the *dump* and *javadump* operations
- `system` is also used to help diagnose the excessive memory consumption and memory leaks, but they are also useful for finding defects in the virtual machine. These dumps are only supported on IBM J9 virtual machines. The resulting file is named `core.date.time.processID.sequenceNumber.dmp`. This value applies to both the *dump* and *javadump* operations.
- `thread` is used to help diagnose hung threads, deadlocks, and can sometimes be used for diagnose excessive CPU issues. These dumps are always created with the `server javadump` command. On IBM J9 virtual machines, the resulting file is named `javacore.date.time.processID.sequenceNumber.txt`. On HotSpot virtual machines, the resulting file is named `javadump.date.time.processID.sequenceNumber.txt`. This value can also be applied to the *dump* operation.

**Note:** The thread dump type is supported only when the server is running on the Java SDK. If the server is started with a JRE, an error is reported indicating that the server does not support the dump type. This restriction applies to HotSpot virtual machines only; the thread Java dump type is supported on any IBM JVM (JRE or SDK).

**8.5.5.0** **--os=os\_value,os\_value,...**

Specifies the operating systems that you want the packaged server to support. Supply a comma-separated list. The default value is `any`, indicating that the server is to be deployable to any operating system supported by the source.

To specify that an operating system is not to be supported, prefix it with a minus sign ("`-`"). For a list of operating system values, refer to the OSGi Alliance web site at the following URL: <http://www.osgi.org/Specifications/Reference#os>.

This option applies only to the *package* operation, and can be used only with the **--include=minify** option. If you exclude an operating system, you cannot later include it if you repeat the *minify* operation on the archive.

## Server Process

The server process is created by using the environment variables that are specified in the `server.env` file. The following JVM options are added by default:

- **8.5.5.0** The `-javaagent:wlp/bin/tools/ws-javaagent.jar` option is required for trace, monitoring, and other server capabilities.
- The `-Xshareclasses` and related options enable the shared class cache on supported IBM J9 virtual machines. The cache directory is set to `WLP_OUTPUT_DIR/.classCache`.
- The `-XX:MaxPermSize` option increases the size of the permanent generation for HotSpot virtual machines prior to Java 8. You can set the `WLP_SKIP_MAXPERMSIZE` environment variable to `true` to avoid this default option, which avoids warnings such as:

Java HotSpot(TM) Client VM warning: ignoring option MaxPermSize=256m; support was removed in 8.0

You can use the `jvm.options` file to override these default JVM options or add additional JVM options. For more information about the `server.env` and `jvm.options` file, see “Customizing the Liberty environment” on page 1565.

**UNIX** **z/OS** **IBM i** **8.5.5.1** By default, the `server` command sets the `umask` value to deny all permissions to “Other” users before running the action. However, you can set the `WLP_SKIP_UMASK` environment variable to `true` to avoid setting the `umask` value.

The current working directory of the server process is set to the server output directory.

**UNIX** **z/OS** **IBM i** The `server` command creates a process ID (PID) file when you start the server and deletes the PID file when you stop the server. By default, the PID file is set to `WLP_OUTPUT_DIR/.pid/serverName.pid`. The absolute path of the PID file can be changed by setting the `PID_FILE` environment variable, or the absolute path of the PID directory can be changed by setting the `PID_DIR` environment variable.

The standard output and error from the server process is output to the foreground console when you use the `run` and `debug` actions and is redirected to the `WLP_OUTPUT_DIR/serverName/logs/console.log` file by default when you use the `start` action. The log name can be changed by setting the `LOG_FILE` environment variable, and the log directory can be changed by setting the `LOG_DIR` environment variable. For more information about the logging configuration, see “Liberty:Logging and Trace” on page 2313.

The `stop` action prevents new application requests from entering the server, which allows existing requests some time to complete. After that time, the remaining server components are stopped and the server process exits. Application requests that do not complete in the allowed time fail, but their exact behavior depends on their activity when the server components stopped.

## Exit codes

The following exit codes are available for the `server` command and the equivalent executable JAR file `ws-server.jar`:

- 0 OK. 0 indicates successful completion of the requested operation. For server status, 0 indicates that the server is running.
- 1 For server status, 1 indicates that the server is not running. For other operations, it indicates invocation of a redundant operation. For example, starting a started server or stopping a stopped server. This code might also be returned by JVM if invalid Java options are used.
- 2 The server does not exist.
- 3 An unsupported action was called on a running server. For example, the server is running when the package action is called.

- 4 An unsupported action was called on a stopped server. For example, the server is not running when the dump action is called
- 5 Unknown server status. For example, the workarea directory is missing, or the Attach API fails to work.
- >=20 Return codes greater than or equal to 20 indicates that an error occurred while performing the requested . Messages are printed and captured in log files with more information about the error.

## Usage

The following examples demonstrate the correct syntax:

```
server run
server start myserver --clean
server package myserver --archive="archivefile.zip" --include=all
server dump myserver --archive="c:\mybackup\myserver.zip" --include=thread
```

8.5.0.1

server javadump myserver

8.5.0.1

server javadump myserver --include=heap,system

## Liberty: iAdmin command

IBM i

The command supports operating a Liberty server on the IBM i platform. The command file is in the wlp/lib/native/os400/bin directory. The command file is a script named iAdmin.

## Syntax

The command syntax is as follows:

```
iAdmin task [options]
```

where the value of **task** can be one of the following options:

- **POSTINSTALL**
- **PREUNINSTALL**
- **GRANTAUTH**

The **POSTINSTALL** task configures the server start command to launch servers as jobs in the QWAS85 subsystem. Additionally, the task:

- Configures Liberty to run servers under the QEJBSVR user profile.
- Configures the default JDK location by setting WLP\_DEFAULT\_JAVA\_HOME in file wlp/etc/default.env to the location of the 32 bit version of the minimum supported Java level.
- Adds an entry for the product in the IBM i native product registry.
- Creates IBM i native libraries and objects such as the QWAS85 subsystem and the QEJBSVR user profile.

Call the iAdmin POSTINSTALL command only after Installing Liberty by extracting an archive file.

The **GRANTAUTH** task grants the QEJBSVR user profile the necessary file permission and ownership for the server role. The **POSTINSTALL** sets the file ownership and authorities correctly for the QEJBSVR user profile. However, if you create files manually, or if you modify the authorities on files used by the Liberty server, you can call the iAdmin GRANTAUTH command to ensure that QEJBSVR has the correct authorities.

The **PREUNINSTALL** task removes the native libraries and objects created by the **POSTINSTALL** task. Call the iAdmin PREUNINSTALL command before removing the Liberty application-serving environment from your system, but you only need do so if Liberty was installed by executing a JAR file.

## Note:

- You must have \*ALLOBJ and \*SECADM special authority to use the **POSTINSTALL** and **PREUNINSTALL** commands.
- You must have \*ALLOBJ special permission, own, or have \*OBJMGT authority to all objects in the specified directory subtrees to use the **GRANTAUTH** command.
- After running the **POSTINSTALL** task, you must also have \*ALLOBJ and \*SECADM special authority to start and stop the Liberty server.

## Options

The following options are available for the **iAdmin** command:

### **--outputdir wlp\_user\_dir**

The directory for server generated files. This option must only be an absolute path, is optional for the **GRANTAUTH** task, and is ignored for all other tasks. When not specified, the default location for server generated output is used.

### **--rolename role\_name**

The role that the user profile is assigned. The server role is the only currently supported role. This option is required for the **GRANTAUTH** task and is ignored for all other tasks.

### **--userdir wlp\_user\_dir**

The directory containing shared resources and server definitions. This option can only be an absolute path, is optional for the **GRANTAUTH** task, and is ignored for all other tasks. When not specified, the default location for shared resources and server definitions is used.

### **--userprofilename user\_profile\_name**

The user profile to grant authority to. **QEJBSVR** is the only currently supported user profile name for the server role. This option is required for the **GRANTAUTH** task and is ignored for all other tasks.

## Usage scenarios

The following examples demonstrate correct syntax. Run the command in any of the following examples on one line.

- Configuring Liberty to start as a job in the QWAS85 subsystem and to swap to the QEJBSVR user profile when running.  
`wlp/lib/native/os400/bin/iAdmin POSTINSTALL`
- Granting the server role to the QEJBSVR user profile for the shared resources, server definitions, and output locations configured for this Liberty runtime environment.  
`wlp/lib/native/os400/bin/iAdmin GRANTAUTH --rolename server --userprofilename QEJBSVR`
- Removing the native libraries and objects created by the **POSTINSTALL** task.  
`wlp/lib/native/os400/bin/iAdmin PREUNINSTALL`

## Liberty:application client commands



8.5.5.6

The **client** command supports create, run, debug, package and help actions.

## Syntax

The `wlp/bin` directory contains scripts that are called `client` and `client.bat` to help with running client applications. The syntax of these scripts are as follows:

```
client <action> client_name [options]
```

where the value of **action** represents the operation that you can perform on an application client.

**Attention:** If an application client name is not specified on the command line, the task is taken against the default application client instance, `defaultClient`.

## Actions

The client script supports the following actions:

**create** A command that creates a new application client.

**run** A command that launches the application client in the foreground.

**debug** A command that runs the named application client in the console foreground after a debugger connects to the debug port. The default port is 7778.

**package** A command that packages an application client.

**help** A command that gets command-line script help, including details of more options.

## Options

The client script supports the following options:

**--archive="path to the target archive file"**

Specify the archive target to be generated by the package action. You can specify the target as an absolute path or as a relative path. If this option is omitted, the archive file is created in the client output directory. The target file name extension might influence the format of the generated archive. The default archive format for the package action is pax on z/OS and zip on all other platforms. The jar archive format produces a self-extracting jar file that similar to the original installer archive.

**--clean**

Clean all cached information related to this client instance.

**--include=value,value,...**

A comma-delimited list of values. The valid values vary depending on the action.

**template="templateName"**

Specify the name of the template to use when creating a new client.

**--autoAcceptSigner**

Automatically accept and store the signer certificate in the client truststore without being prompted to examine the server certificate.

## Example

The following examples show the application client command actions that you can run on Windows systems: 

```
client.bat create client_name
client.bat run client_name
client.bat help
```

The following examples show the application client command actions that you can run on other systems:

```
client create client_name
client run client_name
client help
```

## Running an application client from the command line: 8.5.5.6

You can use the client run task to run an application client.

### Before you begin

Before you can run an application client, you must create a client and add a configuration for your client application in the `client.xml` file. See the [Creating a Liberty client manually](#) topic for examples of how you would create the application client.

### About this task

The `wlp/bin` directory contains scripts that are called `client` and `client.bat` to run client applications. The syntax of these scripts is as follows:

```
client action <client_name> [options]
```

### Procedure

Use the following command to run the client:

```
client run client_name
```

#### Windows

```
client.bat run client_name
```

where *client\_name* is the name of the client.

**Attention:** If a default client exists, it runs `defaultClient`. If a default client does not exist, `defaultClient` is created, then runs (and likely fails because there is no application that is configured).

## Liberty:configUtility command

8.5.5.5

The **configUtility** command enables you to download configuration snippets from the IBM WebSphere Liberty Repository. The command also enables you to replace configuration snippet variables with your input values. The Liberty repository *config snippets* are samples of Liberty server configurations for specific tasks.

For information about accessing and using the Liberty repository, see “[Liberty: Liberty Repository](#)” on page 965.

### Syntax

The command syntax is as follows:

```
configUtility action | configUtility configSnippet [options]
```

where *action* can take one of the following values:

**find** Display a list of all configuration snippets in the repository.

 Specify a string to filter the list to configuration snippets that have the specified string in the description. Enclose strings that contain spaces in double-quotation marks.

**help** Display help information for a specified action.

**install** Download the configuration snippet from the repository or use a local configuration snippet for variable substitution.

The *configSnippet* variable is the name of the configuration snippet. Run the **configUtility find** command to get the names of configuration snippets in the repository.

## Options

The following options are available for the **configUtility install configSnippet** command:

**--info** List all variable options in the configuration snippet. Return an empty list if the configuration snippet has no variables for substitution.

**--v[variable]=value**

Replace configuration snippet variables found by the **--info** option with your input values. The utility identifies these variable using **--v[variable]**. Do not include the brackets ([]) in the command.

**--createConfigFile=path**

Optional. The utility writes the code snippet to the file specified by *path* instead of to the console screen. Add the provided code snippet to the server.xml configuration to include the specified file.

**--encoding=[xor|aes]**

Optional. Specify the keystore password encoding. Supported encodings are xor and aes. The default encoding is xor.

**--key=key**

Optional. Specify a key to be used when encoding using AES. This string is hashed to produce an encryption key which is used to encrypt and decrypt the password. Optionally, provide the key to the server by defining the variable wlp.password.encryption.key whose value is the key. If this option is not provided, a default key is used.

**--useLocalFile=file**

Use a configuration snippet from a local file system. You must specify the file path. This option replaces specifying a configuration snippet name.

## Usage

The following examples demonstrate correct syntax:

```
configUtility find
configUtility find filter_string
configUtility find "filter string"
configUtility help
configUtility install configSnippet
configUtility install configSnippet --info
configUtility install configSnippet --vvariable=value
configUtility install configSnippet --createConfigFile=C:/wlp/usr/servers/server1/snippet-include.xml
configUtility install configSnippet --encoding=aes --key=myAESkey
configUtility install --useLocalFile=C:/wlp_temp/mySnippet.xml
```

**Tip:** If your option value has spaces, you must enclose it in double quotation marks ("). For example, if the file path for the **--createConfigFile** option is C:\Program Files\mySnippets\snippet-include.xml, specify **--createConfigFile="C:/Program Files/mySnippets/snippet-include.xml"** in the command.

## CAUTION:

Different operating system might treat some characters differently. For the Windows environment, if you have ! in your input string, it needs to be escaped by the ^ character. For example,

```
D:\Liberty\images\855\Liberty855\wlp\bin>configUtility createConfigFile="a^!"
```

## Downloading and customizing configuration snippets from the command line: 8.5.5.5

You can use the **configUtility** command to download configuration snippets from the IBM WebSphere Liberty Repository. You can also use the command to replace configuration snippet variables with your input values. The Liberty repository *config snippets* are samples of Liberty server configurations for specific tasks.

### Procedure

1. Open a command line, then change directory to the wlp/bin directory.
2. Generate a list of configuration snippets in the Liberty repository.

Run the following command to write a list of configuration snippets to your console screen:

```
configUtility find
```

From this generated list, you can determine the name of a configuration snippet to download and, optionally, modify.

8.5.5.6 You can specify a string to filter the list to configuration snippets that have the specified string in the description. For example, for a list of security-related configuration snippets, run:

```
configUtility find security
```

Enclose strings that contain spaces in double-quotations marks; for example:

```
configUtility find "ejb security"
```

3. Optional: Generate a list of all variable options for a configuration snippet.  
Using the name of configuration snippet obtained in step 2, run the following command to write a list of variable options for the snippet to your console screen. For *configSnippet*, specify the name of the snippet:

```
configUtility install configSnippet --info
```

The command returns an empty list if the configuration snippet has no variables for substitution.

4. Download a configuration snippet.

Using the name of the configuration snippet obtained in step 2, run the following command to write the configuration snippet to your console screen. For *configSnippet*, specify the name of the snippet:

```
configUtility install configSnippet
```

To write the configuration snippet to a file instead of to your console screen, add the **--createConfigFile** option and specify a file path. You can include the generated file in a server.xml configuration file using an include statement. For example, to write the configuration snippet to the C:\wlp\usr\servers\server1\snippet-include.xml file on your local file system, run the following command:

```
configUtility install configSnippet --createConfigFile=C:\wlp\usr\servers\server1\snippet-include.xml
```

**Tip:** If the file path has spaces, you must enclose it in double quotation marks ("). For example, if the file path is C:\Program Files\mySnippets\snippet-include.xml, specify **--createConfigFile="C:/Program Files/mySnippets/snippet-include.xml"** in the command.

To download and replace configuration snippet variables found by the **--info** option with your input values, use the **--v[variable]=value** option:

```
configUtility install configSnippet --v[variable]=value
```

For example, to specify a value of user1 for the \$[adminUser] variable in the remoteAdministration snippet, run:

```
configUtility install remoteAdministration --vadminUser=user1
```

This command writes a configuration for Remote Administration to a console screen, with user1 replacing the `[$adminUser]` variable:

```
<quickStartSecurity userName="user1" userPassword="{adminPassword}"/>
```

For more information about command options, see “Liberty:configUtility command” on page 1575.

## Running the ddlGen utility

8.5.5.6

You can generate data definition language (DDL) if there are features in the server configuration that require access to a database.

### Before you begin

You must start the server before running the ddlGen utility.

### About this task

The utility generates data definition language (DDL) for each feature that is configured in the server that requires access to a database. You can change the path that the ddlGen utility uses to search for the server by exporting the environment variable, `WLP_USER_DIR`, in the command line where the utility is run.

### Procedure

1. In the `server.xml` file, add the `localConnector-1.0` feature under the `featureManager` tag.

```
<featureManager>  
  <feature>localConnector-1.0</feature>  
</featureManager>
```

2. In a command line, run the `wlp/bin/ddlGen {generate|help} <server_name>` command, where `<server_name>` is the name of the server that you want to generate DDL for.

### Results

The following table shows the nonzero codes that might be returned:

Table 117. Return codes and explanations for the ddlGen utility

Return Code	Explanation
0	Success. The DDL is generated to <code>/\${server.output.dir}/ddl</code> .
20	The action provided is not valid.
21	The server was not found. Message CWWKD0100E shows the file system directory where the utility looked for the server. This location can be changed by exporting the variable, <code>WLP_USER_DIR</code> , in the command line where the utility is run.
22	The <code>localConnector</code> feature is not present in the server configuration or the server was not started.
23	The MBean that generates DDL was not found.
24	The MBean that generates DDL reported an error. The server logs contain more details about the error.
255	An unexpected error occurred.

## Liberty:Generating Liberty configurations schema from the command line

8.5.5.0

Use the `ws-schemagen.jar` tool that is in the installation's `bin/tools` directory to generate the schema for Liberty core and other installed products extensions in a single output file.

## Syntax

The command syntax is as follows:

```
java [JVM options] -jar ws-schemagen.jar [options] outputFile
```

## Options

The following options are available:

### **--encoding=charset**

Where *charset* is the character set to use when you are creating the output file.

### **--ignorePidsFile=fileName**

Where *fileName* is the name of the file name that contains a list of pids to ignore.

### **--locale=language**

Where *language* specifies the language to use when you are creating the output file. This string consists of the ISO-639 two-letter lowercase language code, optionally followed by and underscores and the ISO-3166 uppercase two-letter country code.

## Usage examples

The following example generates the installed products' schema and stores in a file called `schema.xml`:

```
java -jar ws-schemagen.jar schema.xml
```

The following example generates the installed products' schema and stores in a file that is called `schema.xml` using the Brazilian Portuguese language:

```
java -jar ws-schemagen.jar schema.xml --locale=pt_BR
```

The following example displays help information:

```
java -jar ws-schemagen.jar --help
```

## Generating a Liberty server dump from the command line

From the command line, you can use the `server dump` **8.5.0.1** or `server javadump` command to capture status information for a Liberty server.

### About this task

The `server dump` command is useful for problem diagnosis of a Liberty server because the result file contains server configuration, log information, and details of the deployed applications in the `workarea` directory. The command can be applied to either a running or a stopped server.

For a running server, the following information is also included:

- State of each OSGi bundle in the server
- Wiring information for each OSGi bundle in the server
- Component list that is managed by the Service Component Runtime (SCR) environment
- Detailed information of each component from SCR
- Configuration administration data of each OSGi bundle
- Information about registered OSGi services
- Runtime environment settings such as Java virtual machine (JVM), heap size, operating system, thread information, and network status

**8.5.0.1** The server `jvaddump` command is useful for diagnosing problems at the JVM level, such as hung threads, deadlocks, excessive processing, excessive memory consumption, memory leaks, and defects in the virtual machine. The command can be used only on a running server. Each dump type creates a file, but not all dump types are supported by all virtual machines. See “Liberty:server command options” on page 1569. The default directory for dump files is `${server.output.dir}`. To set a different default directory, you must use an IBM JVM and set the following environment variables:

- **IBM\_HEAPDUMPDIR**
- **IBM\_COREDIR**
- **IBM\_JAVACOREDIR**

## Procedure

1. Open a command line, then change directory to the `wlp/bin` directory.
2. **8.5.0.1** Capture the status information by using one of the following command-line tools. If you do not specify a server name, `defaultServer` is used.
  - To create a snapshot of the server status, use `server dump` command.

**Distributed operating systems** **IBM i**

```
server dump server_name --archive=package_file_name.dump.zip
```

**8.5.0.1** `--include=heap` where `package_file_name.dump.zip` is a file name that you choose. This file name can include a full path name. If the full path is omitted, a compressed file called `package_file_name.dump.zip` is created in default directory `${server.output.dir}`.

**z/OS**

```
server dump server_name --archive=package_file_name.dump.pax
```

**8.5.0.1** `--include=heap` where `package_file_name.dump.pax` is a file name that you choose. This file name can also include a full path. If the full path is omitted, a compressed file called `package_file_name.dump.pax` is created in default directory `${server.output.dir}`.

**8.5.0.1** The `--include` parameter is optional. You can request additional memory dump types. For example, `--include=heap` option requests a heap dump; `--include=thread,heap,system` option requests a thread dump, a heap dump, and a system dump.

- **8.5.0.1** To create a snapshot of the JVM status, use `server jvaddump` command.

**Distributed operating systems** **IBM i**

```
server jvaddump server_name --include=heap
```

**z/OS**

```
server jvaddump server_name --include=heap
```

The `--include` parameter is optional. You can request additional memory dump types. For example, `--include=heap` option requests a heap dump; `--include=heap,system` option requests a heap dump and a system dump. The output files are created in the default directory `${server.output.dir}`. To set a different default directory, you must use an IBM JVM and set the **IBM\_HEAPDUMPDIR**, **IBM\_COREDIR**, and **IBM\_JAVACOREDIR** environment variables.

**Note:** The resulting file is created by using UTF-8 encoding for entry names, so the tool that you use to open the file must be able to use UTF-8 encoding for entry names. The `jar` command in a Java SDK uses this format.

## Results

If the specified server does not exist, the command does not succeed. If the specified server exists, a result file is created that contains the status information of the server.

## Packaging a Liberty server from the command line

From the command line, you can create a compressed file that contains a Liberty runtime environment, the files in the shared resources directory, a specific server, and the applications that are embedded in the server. You can also choose to exclude the runtime binary files from the compressed file.

### About this task

The Liberty server is lightweight, and therefore you can easily package a server installation in a compressed file. You can store this package, distribute it to colleagues, and then use it to deploy the installation to a different location or to another machine, or even embed the installation in a product distribution.

The server installation that you want to package cannot already be joined to a collective. You can only package a stand-alone server.

**Note:** **Distributed operating systems** The resulting file is created by using UTF-8 encoding for entry names, so the tool that you use to open the file must be able to use UTF-8 encoding for entry names. The `jar` command in a Java SDK uses this format.

### Procedure

To package a Liberty server from the command line, complete the following steps:

1. Open a command line, then change directory to the `wlp/bin` directory.
2. Stop the server.
3. Run the **package** command to create a package.

**8.5.5.5** You can package the Liberty profile server or the runtime.

- Package the Liberty server.

The default archive format is `.zip` on all platforms apart from z/OS where it is `.pax`. You can also generate a `.jar` archive.

If you do not specify a server name, `defaultServer` is used. If you do not specify the **--archive** parameter, the value of `server_name` is used for `package_file_name`, and the compressed file is created in the `${server.output.dir}` directory.

Choose the correct command for your environment.

– **Distributed operating systems** **IBM i**

Use this command to generate a `.zip` archive.

```
server package server_name --archive=package_file_name.zip --include=all
```

where `package_file_name.zip` is a file name that you choose. This file name can include a full path name. If the full path is omitted, a compressed file called `package_file_name.zip` is created in the `${server.output.dir}` directory.

– **Distributed operating systems** **IBM i**

Use this command to generate a `.jar` archive. The advantage of a `.jar` archive is that the scripts in the `bin` directory keep their permissions, so they are executable when the package is installed.

```
server package server_name --archive=package_file_name.jar --include=all
```

where `package_file_name.jar` is a file name that you choose.

For more information about extraction options with this archive file, see “Java archive file extraction options” on page 1376.

– **z/OS**

Use this command to generate a `.pax` archive.

```
server package server_name --archive=package_file_name.pax --include=all
```

where *package\_file\_name.pax* is a file name that you choose. This file name can also include a full path. If the full path is omitted, a compressed file called *package\_file\_name.pax* is created in the `${server.output.dir}` directory.

The pax archive format saves the extended attributes that are required for the Liberty to work as designed in all supported scenarios. If a compressed file in ZIP format is required, specify the target archive name and include the `.zip` extension. If the specified name ends with `.zip`, then a compressed file in ZIP format is generated, instead of the z/OS default PAX format.

An archive format of `.jar` is not valid on z/OS.

You can also use the `--include` option with this command. For example, the `--include=all` option packages the runtime binaries and the relevant files in the `${WLP_USER_DIR}` directory; the `--include=usr` option packages only relevant files in the `${WLP_USER_DIR}` directory, effectively excluding the runtime binaries from the compressed file.

The `--include=usr` option is not valid with an archive format of `.jar`.

**8.5.5.0** If you use the `--include=minify` option, the **server** command packages only those parts of the runtime environment, and files in the `${WLP_USER_DIR}` directory, that are required to run the server. This option significantly reduces the size of the resulting archive.

The parts of the runtime environment that are retained by the `minify` operation depend on the features that are configured in the server that you are packaging. Only those features that are required to run the server are retained, and the remaining features are removed. Therefore, you cannot later enable a feature that has been removed. For example, if only the `servlet-3.0` feature is retained, you cannot later enable the `jpa-2.0` feature.

You can repeat the `minify` operation to further reduce the size of the archive if the configuration is changed. There is, however, no reverse operation for the `minify` operation, so if you later require one or more features that have been removed, you must begin again with a complete Liberty server.

While the `minify` operation is running, the server is temporarily started, and you see the associated messages. For this reason, you cannot use the `--include=minify` option with a server that is not able to be started, but you can package it with the `--include=all` or `--include=usr` options.

You can specify the operating systems that you want the packaged server to support by using the `--os` option with the `--include=minify` option.

For example, to package a server with z/OS support removed, use the following command:

```
server package --archive="nozoz.zip" --include=minify --os=-z/OS
```

To package a server with OS/400 support retained, but z/OS support removed, use the following command:

```
server package --archive="small.zip" --include=minify --os=OS/400,-z/OS
```

To package a server that supports only Linux, use the following command:

```
server package --archive="linux.zip" --include=minify --os=Linux
```

**Note:** **z/OS** To unpackage a file on z/OS, go to the location where you want to unpackage the file and then run the following command. The `-ppx` option is used to preserve the extended attributes.

```
pax -ppx -rf location filename.pax
```

Where *location* is the path where the file exists and *filename.pax* is the name of the file.

- **8.5.5.5** Package the Liberty runtime.

Create a runtime archive that contains the `wlp` directory, but does not contain the `usr` directory. The naming convention for a server package is *package\_name.zip*; for example, `CustomerPortalApp.zip`. To create a runtime archive, run the **package** command without a server name and with the `--include=wlp` option:

```
server package --include=wlp
```

To specify a package file name and target location, add the `--archive=package_path_name` option; for example:

```
server package --include=wlp --archive=c:\temp\myPackage.zip
```

If you do not specify a valid package name or target location with the `--archive` option, then the command creates the `wlp.zip` runtime archive in the `$WLP_OUTPUT_DIR` location, which is the `${wlp.install.dir}/usr/servers` directory by default. The target location must exist before running the command. Thus, if the target location is `c:\temp`, the `C:\temp` directory must exist and have write permission for the command to write the archive to the `C:\temp` directory.

## Running a Liberty server from a JAR file

8.5.5.9

You can start a Liberty server from a Java archive (JAR) file. This method provides a compact, portable way of starting a Liberty server. You create the JAR file by using the Liberty server command and then run as an executable JAR file by using the `java -jar` command.

### Create the runnable JAR file

You can specify `minify` to get the smallest archive possible. You must specify a JAR type archive to get a runnable JAR file. The default archive type is `.zip` on all platforms except `z/OS`, where the only supported type is `pax`. For example:

```
server package <server name> --include=[minify,]runnable --archive=<jar file name>.jar
```

### Run the JAR file

Run the JAR file by using the standard `java` command with the `-jar` option, for example:

```
java -jar <jar file name>.jar
```

### Operation

When the JAR file runs, it gets extracted to a temporary location and then the server runs in the foreground, started by the Liberty server run command. All output is written to `stdout` or `stderr`. By default, files are extracted to temporary locations:

- For Windows: `%HOMEPATH%/wlpExtract/<jar file name>_nnnnnnnnnnnnnnnnnn`
- For all other platforms: `$HOME/wlpExtract/<jar file name>_nnnnnnnnnnnnnnnnnn`

You can control the output location by using the `WLP_JAR_EXTRACT_ROOT` or `WLP_JAR_EXTRACT_DIR` environment variable.

### Stopping the server

To stop the Liberty server press **Ctrl-C**. When the Liberty server stops, the extraction directory is automatically deleted. If you stop the active shell in any other way, the extraction directory is not cleaned up automatically, you must clean it up manually.

### Run in debug mode

You can run the Liberty server in debug mode if you set the environment variable `WLP_JAR_DEBUG` before you start the server.

### Controlling output

By default, server output is written to the extraction directory, which is deleted when the server stops. If you want to save the output, specify a durable output location by using the `WLP_OUTPUT_DIR` environment variable before you start the server.

## Two-phase commit transactions

By default, two-phase commit transactions are disabled because the transaction logs are in the expansion directory and are deleted when the Liberty server is stopped. Therefore, transaction recovery is not possible.

To enable two-phase commit, configure the transaction log to be in a durable location in the file system or an RDBMS and set the `WLP_JAR_ENABLE_2PC` environment variable.

To configure the transaction log, use either the `transactionLogDirectory` or `dataSourceRef` attribute on the transaction element in your `server.xml` configuration.

## Running under CYGWIN

Running a Liberty server JAR file in a CYGWIN shell has two requirements:

1. Specify the `WLP_JAR_CYGWIN` environment variable.

This variable causes the Liberty server JAR runner to do UNIX-style file and process handling when it is running in the CYGWIN environment.

2. Run under the bash shell, not mintty.

Automatic extraction file deletion occurs only when you run under the bash shell. You can run under mintty, but you must delete the extraction files manually. Mintty does not forward the necessary signal that is required to trigger Java shutdown hooks.

## Environment variable reference

Table 118. The environment variable names and their definitions

Environment variable name	Description
<code>WLP_JAR_EXTRACT_ROOT</code>	Extracts JAR file to directory <code>\${WLP_JAR_EXTRACT_ROOT}/&lt;jar file name&gt;_nnnnnnnnnnnnnnnnnnnn</code>
<code>WLP_JAR_EXTRACT_DIR</code>	Extracts JAR file to directory <code>\${WLP_JAR_EXTRACT_DIR}</code> .
<code>WLP_OUTPUT_DIR</code>	Writes Liberty server output files to directory <code>\${WLP_OUTPUT_DIR}</code> .
<code>WLP_JAR_DEBUG</code>	Runs Liberty server by using server debug <code>&lt;server name&gt;</code> instead of server run <code>&lt;server name&gt;</code> .
<code>WLP_JAR_ENABLE_2PC</code>	Set to value true to enable 2PC when the runnable JAR file runs.
<code>WLP_JAR_CYGWIN</code>	Set to value true if you are running the JAR file under CYGWIN.

## Starting and stopping a server from the command line

You can use the server tasks to start or stop a server.

### About this task

The `wlp/bin` directory contains a script called `server` to help with controlling the server process. The syntax of this script is as follows:

```
server action serverName [options]
```

For available values of `[options]`, see “Liberty:server command options” on page 1569.

**Note:** If a server is not specified on the command line, the action is performed against the default server instance, `defaultServer`, if it exists.

**Tip:** Do not use the command line to start or stop a server that is managed by auto scaling with an enabled scaling policy.

## Procedure

- Use the following command to start the server:

```
server start serverName
```

where *serverName* is the name of the server.

- Use the following command to stop the server:

```
server stop serverName
```

where *serverName* is the name of the server.

**Note:** Normal server stop includes a quiesce stage before the server is shutdown. The quiesce stage, a period of 30 seconds, allows for services to perform pre-shutdown work, for example, stopping inbound listeners while allowing existing requests to complete. Applying the `--force` option to the stop command will skip the quiesce stage. The `--force` option will have no effect if **server stop** was already invoked. If you use the `--force` option, you may see unexpected exceptions in the `messages.log` file that occur after the **server stop** command was received by the server.

## Example

To start or stop a server by using the server script on Windows systems:

```
server.bat start serverName
```

```
server.bat stop serverName
```

To start or stop a server by using the server script on other systems:

```
server start serverName
```

```
server stop serverName
```

## Starting and stopping a Liberty server as a Windows service

### Windows

You can optionally register the Liberty server as a Microsoft Windows Service program when you run on Windows operating systems. You can manually start, stop, and unregister the Liberty server as a Windows service. You can also use the Microsoft Windows Services program to change Liberty to start automatically as a Windows service when the Windows server starts.

## Before you begin

Set the `JAVA_HOME` environment variable before you run the following commands. You can use the `server.env` file path to set the `JAVA_HOME` value reliably. For more information about using the `server.env` file, see “Customizing the Liberty environment” on page 1565.

## About this task

The commands to register, start, stop, and unregister Liberty as a Windows service use the same `server.bat` file that is used when you start the Liberty server from the command line. For available values of `[options]`, see “Liberty:server command options” on page 1569.

## Procedure

- Use the following command to register the server:

```
server registerWinService serverName
```

where *serverName* is the name of the server.

The Windows service name and Windows service display name is the *serverName*. After you register, you can find and administer the Liberty server as a service by using **regedit** from the Windows Registry program. Entries for the service in the registry are in the following locations:

```
HKEY_LOCAL_MACHINE->SOFTWARE->Wow6432Node->Apache Software Foundation->Procrun 2.0->serverName
HKEY_LOCAL_MACHINE->SYSTEM->CurrentControlSet->services->serverName
```

- Use the following command to start the server:

```
server startWinService serverName [options]
```

where *serverName* is the name of the server.

- Use the following command to stop the server:

```
server stopWinService serverName
```

where *serverName* is the name of the server.

- Use the following command to unregister the server:

```
server unregisterWinService serverName
```

where *serverName* is the name of the server.

## What to do next

When you install a fix pack by using archives, the directory under which the fix pack is installed can change from the directory where the Liberty server was running before you installed the fix pack. If you are running a Liberty server as a Windows service, then unregister that Liberty server as a Windows service before you install the fix pack. After you install the fix pack, register the Liberty server as a Windows service again.

If you need to manually remove Liberty as a Windows service, then update the Windows registry by using the Windows **regedit** program. The two entries that need to be removed from the Windows Registry are in the following locations:

```
HKEY_LOCAL_MACHINE->SOFTWARE->Wow6432Node->Apache Software Foundation->Procrun 2.0->serverName
HKEY_LOCAL_MACHINE->SYSTEM->CurrentControlSet->services->serverName
```

## Using Ant to automate tasks for Liberty

Apache Ant is a Java library tool for automating the build process. You can use Ant tasks that are provided by Liberty to manage the server and applications.

### Before you begin

**Important:** The `wlp-anttasks.jar` file that is included with Liberty is planned to be removed. For more information, see Removal notices. An open source Ant plug-in with more tasks for Liberty is available. The more recent Ant plug-in has a different antlib namespace, `xmlns:wlp="antlib:net.wasdev.wlp.ant"`. For more information about the open source Ant plug-in for Liberty, see the GitHub repository.

The Liberty Ant plug-in `wlp-anttasks.jar` files are located in Maven Central. If you want to use these tasks in your build script, you must make sure the plug-in is available on the Ant class path. Copy the plug-in file `wlp-anttasks.jar` to the `/lib` directory of the Ant installation, and declare the `antlib` namespace in the `build.xml` file. See the following example:

```
<project .... xmlns:wlp="antlib:net.wasdev.wlp.ant">
  ...
</project>
```

The namespace can be any string, provided you avoid name conflicts. After that, you must use the namespace as a prefix of the Ant tasks for Liberty. For example, you must use `wlp:server` when calling the server task.

## About this task

You can create build scripts that use these Ant tasks to package, install, and test your application on Liberty.

## Using an OSGi console

Eclipse Equinox currently provides an OSGi console that you can use to aid with debugging. This console is not available by default. You can enable this console in the OSGi framework that is running within Liberty by using the `osgiConsole-1.0` feature and by specifying a port to attach to.

## About this task

Liberty uses the Eclipse Equinox implementation of the OSGi core specification. Equinox currently provides an OSGi console. To enable this console, you first allocate a specific port to it by setting the `osgi.console` property in the `bootstrap.properties` file. Then you can use Telnet to connect to the console on that port, and explore the OSGi framework.

## Procedure

- **8.5.5.0** Add the `osgiConsole-1.0` Liberty feature to your `server.xml` file.  

```
<feature>osgiConsole-1.0</feature>
```
- Allocate a specific port to the OSGi console.  
You set the OSGi console port by specifying the `osgi.console` property. You set this property as a bootstrap property in the `bootstrap.properties` file. See “Specifying Liberty bootstrap properties” on page 1437.  

```
osgi.console=5471
```

The OSGi console is disabled when the `osgi.console` property is not set.
- Use Telnet to connect to the OSGi console port.  

```
telnet localhost 5471
```
- Use the console to explore the framework.  
The available commands vary, depending on the OSGi framework being used. Command-line help provides enough information to get started.

## Adding and removing Liberty features

Features are the units of functionality by which you control the pieces of the runtime environment that are loaded into a particular server. To add or remove a Liberty feature, you add or remove an XML snippet in the `<feature>` subelement of the `server.xml` configuration file. When you add or remove Liberty features, the changes are applied dynamically.

### Distributed operating systems

## Before you begin

You can add and remove Liberty features as described in this topic, or as described in “Editing the Liberty configuration by using developer tools” on page 1556.

## About this task

For a list of the main Liberty features, including the XML snippets that enable them, see “Liberty features” on page 826.

## Procedure

To add or remove Liberty features, complete the following steps:

1. Open the `server.xml` configuration file for editing.

Where *path\_to\_liberty* is the location you installed Liberty on your operating system, and *server\_name* is the name of your server.

You can do this using a text editor. By default, the path and file name for the configuration root document file is *path\_to\_liberty/wlp/usr/servers/server\_name/server.xml*. However, you can change the path. See **8.5.0.1** “Customizing the Liberty environment” on page 1565.

2. Add or remove features in the configuration file.

The set of features is enclosed within the `<featureManager>` element, and each feature within the `<feature>` subelement. For example:

```
<server>
  <featureManager>
    <feature>servlet-3.0</feature>
    <feature>localConnector-1.0</feature>
  </featureManager>
</server>
```

The matching of feature names is not case-sensitive; the following example is also a valid server configuration:

```
<featureManager>
  <feature>Servlet-3.0</feature>
  <feature>localConnector-1.0</feature>
</featureManager>
```

3. Save the changes to the configuration file.

## Results

Your changes are applied. If the server is running, the changes are applied dynamically.

## Using include elements, variables, and Ref tags in configuration files

You can keep all your configuration settings in a single `server.xml` file, or you can use include elements to consolidate configuration settings from separate files. You can use variables in the configuration to avoid hardcoding values that might not be appropriate when the configuration is reused in different environments. You can use Ref tags to refer to (and thereby reuse) existing code blocks that are defined elsewhere in the configuration.

## Procedure

- “Using include elements in configuration files”
- “Using variables in configuration files” on page 1590
- “Using Ref tags in configuration files” on page 1592

## Using include elements in configuration files

You can keep all your configuration in a single `server.xml` file, or you can use include elements to consolidate configurations from separate files to create the structure that is most useful to you.

## About this task

It can be easier to maintain a complex configuration by splitting it across a set of files. For example:

- You might want to include a file that contains variables that are specific to the local host, so that your main configuration can be used on multiple hosts.

- You might want to keep all of the configuration for a particular application in a separate file that can be versioned with the application itself.

## Example

This is the syntax for including a configuration file. You can set the **optional** attribute as true if you want to skip the include file when it cannot be found :

```
<include optional="true" location="pathname/filename" />
or
<include optional="true" location="url" />
```

The following list shows the possible locations; they are searched in the order shown.

1. in a location specified relative to the parent file
2. in the server configuration directory
3. in a location specified as an absolute path
4. on a web server

To ensure that your include configuration behaves predictably, you need to be aware of the following processing rules for included configuration files:

- For singleton services such as logging, or application monitoring, entries are processed in the order they appear in the file and later entries add to or override previous ones. This is also true for configuration instances, for example an application or data source, where the configuration instances have the same ID.
- Include statements can be placed anywhere within the `<server />` element.
- Each included file must contain a `<server />` element that matches the one in the parent configuration file.
- Included files can nest other included files.
- Each included file is logically merged into the main configuration at the position that the `<include />` statement occurs in the parent file.

In the following example, the primary server configuration file `server.xml` includes the contents of the `blogDS.xml` configuration file, which is located in the shared configuration directory. The `blogDS.xml` file contains a data source definition. This definition has been put in a separate configuration file so that it can be included in several different `server.xml` files, and thereby used across multiple server instances.

Here is example code from the `server.xml` file:

```
<server>
  <featureManager>
    <feature>servlet-3.0</feature>
    <feature>jdbc-4.0</feature>
  </featureManager>
  <application id="blog" location="blog.war" name="blog" type="war"/>
  <include optional="true" location="{shared.config.dir}/blogDS.xml"/>
</server>
```

Here is the example code from the `blogDS.xml` file:

```
<server>
  <dataSource id="blogDS" jndiName="jdbc/blogDS" jdbcDriverRef="derbyEmbedded">
    <properties createDatabase="create" databaseName="C:/liberty/basics/derby/data/blogDB" />
  </dataSource>
  <jdbcDriver id="derbyEmbedded"/>
  <library>
```

```

        <fileset dir="C:/liberty/basics/derby" includes="derby.jar" />
    </library>
</jdbcDriver>
</server>

```

## Using variables in configuration files

You can use variables in the configuration to avoid hardcoding values that might not be appropriate when the configuration is reused in different environments.

### About this task

Variables can be defined by setting a property in any of the following places:

- in the server configuration file, or an included file
- in the `bootstrap.properties` file

The following predefined variables can be referenced:

- directory properties, see “Liberty:Directory locations and properties” on page 1434
- JVM system properties
- **8.5.5.0** process environment variables

If the same variable is specified in multiple places, the precedence is as follows:

- variables in `bootstrap.properties` override the process environment variables
- variables in `server.xml`, or included XML files, override the variables in `bootstrap.properties` and process environment variables

**Best practice:** Variables that are specific to a particular server, for example port numbers, are specified in the `bootstrap.properties` file, allowing the `server.xml` to be shared across multiple servers while you keep those values different in each server. Variables that are shared across a group of servers, for example database configuration for a particular host, is better specified in an xml file that is included into the parent configuration file.

**Best practice:** Variable names must begin with an alphabetic character, and must contain the following characters only: alphabetic characters, numeric characters, and the “\_” and “.” characters.

### Procedure

- Specify a variable in a configuration file.

The variable definition syntax is `variable_name=value`. If the value contains a path, it is normalized during configuration processing by replacing repeated forward and backward slashes with a single forward slash, unless the value starts with double forward or backward slashes, which remain unchanged.

**Best practice:** If you need to set the value of a variable to contain repeated forward slashes, as are sometimes used for JDBC driver connection URLs, break the value into two parts at the double slashes. By placing the double forward slashes as the initial characters, normalization is avoided. For example, to store the value “jdbc:db2://host\_name.com”, use two variables:

```

URL_PART_1="jdbc:db2:"
URL_PART_2="//host_name.com"

```

Variables that are defined in the configuration files are scoped to the configuration elements by which they are used. For example, the following code fragment creates a variable that is called `updateTrigger_var` to be used in **applicationMonitor** configuration elements:

```

<applicationMonitor updateTrigger_var="mbean" />

```

To create a variable that is used in a particular configuration instance (such as an application or resource entry), you must also specify the instance identifier. For example: `<httpEndpoint id="defaultHttpEndpoint" HTTP_default_var="8889" />`

- Specify a variable in the `bootstrap.properties` file.

Variables that are defined in the `bootstrap.properties` file are not scoped to particular configuration elements. You enter the variables as key-value pairs. For example:

```
HTTP_default_var=8006
```

- Use a defined variable in the configuration.

The variable substitution syntax is `${variable_name}`. Multiple variable values may be concatenated by specifying `${variable_name1}${variable_name2}`. For example, to use the `HTTP_default_var` variable, add the following code fragment to the configuration file:

```
<httpEndpoint id="defaultHttpEndpoint"
httpPort="${HTTP_default_var}">
</httpEndpoint>
```

- Use variable element in the configuration

You can use the variable element to define a variable globally in the server configuration. If the same variable is defined in an included file, it is overridden by the one in the `server.xml` file. For example, to use the variable element, add the following code fragment to the configuration file:

```
<variable name="HTTP_default_var" value="8889" />
```

- **8.5.5.0** Use process environment variables in the configuration

Process environment variables are available if you use the `env.` configuration variable prefix, for example:

```
<fileset dir="${env.LIBRARY_DIR}" includes="*.jar"/>
```

For more information about specifying environment variables, see “Customizing the Liberty environment” on page 1565.

- **8.5.5.4** Use variable expressions in configuration

For configuration variables, you can use a limited variable expression syntax with the format `${<operand><operator><operand>}`. The description of the variable is as follows:

#### operand

Operands can either be long integer literals or the name of a variable that contains a long integer value. Variable names must begin with an alphabetic character, and must contain the following characters only: alphabetic characters, numeric characters, and the “\_” and “.” characters.

#### operator

The available operators are as follows:

- + for addition
- - for subtraction
- \* for multiplication
- / for division

If the expression cannot be parsed, a non-integer value is used, or an arithmetic error occurs, then the behavior is undefined.

For example, if the `HTTP_port_base` variable is defined, a variable expression might be used to define multiple `httpEndpoints`:

```
<httpEndpoint id="defaultHttpEndpoint" httpPort="${HTTP_port_base+0}"/>
<httpEndpoint id="httpEndpoint2" httpPort="${HTTP_port_base+1}"/>
```

- Override inheritable attributes in the configuration

You can override the default values of inheritable attributes in the configuration. The inheritable attributes are listed on the page with an `Inherits` type. For example, the **onError** attribute is one of

inheritable attributes. You can define a variable name for the **onError** attribute globally by either setting it in the `bootstrap.properties` or `server.xml` file with a variable element. If the same variable name is specified in both files, the value in the `server.xml` file is used. If the attribute is not explicitly set in either of two files, it uses the default value. If an invalid value is set to the inheritable attribute, the attribute value falls back to the global value defined in `bootstrap.properties` or `server.xml` file or the default value if not defined at the global level.

Another example is logging properties in Liberty. See “Liberty:Logging and Trace” on page 2313.

## Using Ref tags in configuration files

You can define a common configuration element, then reuse that definition by referring to it (using a Ref tag) from elsewhere in the configuration. Ref tags can be used in the same configuration file that contains the element definition, or in an included configuration file.

### About this task

Different approaches are used to specify relationships between the required configuration elements. For example, the following data source definitions are all valid. The first uses no Ref tags, the second uses a combination of direct element definition and Ref tags, and the third uses Ref tags only.

### Example

Example 1: Using no Ref tags.

```
<dataSource id="blogDS" jndiName="jdbc/blogDS">
  <properties createDatabase="create" databaseName="C:/liberty/basics/derby/data/blogDB"/>
  <jdbcDriver>
    <library>
      <fileset dir="C:/liberty/basics/derby" includes="derby.jar"/>
    </library>
  </jdbcDriver>
  <connectionManager maxPoolSize="10"/>
</dataSource>
```

Example 2: Combining direct element definition and Ref tags.

```
<dataSource id="blogDS" jndiName="jdbc/blogDS" connectionManagerRef="derbyPool">
  <properties createDatabase="create" databaseName="C:/liberty/basics/derby/data/blogDB"/>
  <jdbcDriver libraryRef="derbyLib"/>
</dataSource>

<connectionManager id="derbyPool" maxPoolSize="10"/>

<library id="derbyLib"/>
  <fileset dir="C:/liberty/basics/derby" includes="derby.jar"/>
</library>
```

Example 3: Using Ref tags only (except for the properties element, which is only permitted as nested).

```
<dataSource id="blogDS" jndiName="jdbc/blogDS"
  connectionManagerRef="derbyPool" jdbcDriverRef="derbyEmbedded">
  <properties createDatabase="create" databaseName="C:/liberty/basics/derby/data/blogDB"/>
</dataSource>

<connectionManager id="derbyPool" maxPoolSize="10"/>

<jdbcDriver id="derbyEmbedded" libraryRef="derbyLib"/>

<library id="derbyLib" filesetRef="derbyFileset"/>

<fileset id="derbyFileset" dir="C:/liberty/basics/derby" includes="derby.jar"/>
```

## Using the configuration dropins folder to specify server configuration

8.5.5.5

You can specify additional configuration files in the `configDropins` directory without specifying include elements in the `server.xml` file.

### Procedure

1. Create a `configDropins` directory under the `usr/servers/server_name` directory.
  - `usr/servers/server_name/configDropins/overrides`  
If you want to add configuration files to replace anything in the `server.xml` file of the server, create a `configDropins/overrides` directory. For example, to change ports that are defined in the `server.xml`, use a `configDropins/overrides` directory.
  - `usr/servers/server_name/configDropins/defaults`  
If you want the `server.xml` file to be the master configuration, but want to specify defaults for elements that the `server.xml` does not define, create a `configDropins/defaults` directory. For example, if you want developers to be able to provide configuration, but you want the `server.xml` to be the master configuration and you do not want the `server.xml` changed, use a `configDropins/defaults` directory.
2. Place the server configuration files in either the `configDropins/overrides` or `configDropins/defaults` directory.  
Both directories are monitored for updates so that when you add, remove, or update configuration files, the runtime configuration is updated dynamically.  
If there are any conflicts, the following rules determine precedence:
  - The configuration that is specified in the `configDropins/overrides` directory takes precedence over the configuration in the `server.xml` file. Configuration specified in `server.xml` file takes precedence over configuration that is specified in the `configDropins/defaults` directory.
  - Configuration from files in both the `configDropins/defaults` and `configDropins/overrides` directories take precedence over any default configuration that is specified by a feature.
  - The configuration files in the dropins directory are processed in alphabetical order. A later configuration overrides an earlier one. As an example, if `configDropins/defaults` contains `a.xml`, `b.xml` and `c.xml`, the configuration from `c.xml` takes precedence over `b.xml`, and `b.xml` takes precedence over `a.xml`.

**Note:** To maintain consistency across platforms, file names are converted to lower case before sorting alphabetically. This means that if two files are specified in the same dropins directory that have the same name except for case variations (such as `extraConfig.xml` and `ExtraConfig.xml`), the ordering behavior is indeterminate.

3. Optional: Turn off configuration monitoring. See “Controlling dynamic updates” on page 1594.

### ID variables that refer to configuration files

8.5.5.6

The Liberty run time occasionally needs to refer to a configuration element from the `server.xml` file. This action can occur in several ways, such as in the text of a message or in a file name.

The Liberty run time uses an xpath-style syntax to refer to configuration elements. The element type is printed first, followed by brackets that contain the ID of the configuration element. If the configuration element is nested inside another configuration element, the inner configuration element is preceded with a forward slash separating the inner and outer elements.

- For example, the following `databaseStore` configuration element is referred to as `databaseStore[DBTaskStore]` because the `databaseStore` is not nested and has an ID value of `DBTaskStore`.

```
<server>
  <databaseStore id="DBTaskStore">
    ...
  </databaseStore>
</server>
```

- The following data source configuration element is referred to as `databaseStore[DBTaskStore]/dataSource[DataSource0]` because the data source is nested underneath `databaseStore`, `databaseStore` has an ID value of `DBTaskStore`, and data source has an ID value of `DataSource0`.

```
<server>
  <databaseStore id="DBTaskStore">
    <dataSource id="DataSource0">
      ...
    </dataSource>
  </databaseStore>
</server>
```

- In some cases, a configuration element does not have an ID. In this case, an ID is generated. For example, the following data source configuration element might be referred to as `databaseStore[default-0]/dataSource[DataSource0]` because the `databaseStore` does not define an ID.

```
<server>
  <databaseStore>
    <dataSource id="DataSource0">
      ...
    </dataSource>
  </databaseStore>
</server>
```

## Controlling dynamic updates

There are three types of dynamic update that can be controlled through configuration: changing the server configuration; adding and removing applications; updating installed applications. For all deployed applications, you can configure whether application monitoring is enabled and how often to check for updates to applications. For the “dropins” directory, you can also configure the name and location of the directory and choose whether to deploy the applications that are in the directory.

### About this task

By default, deployed applications are monitored for updates, and the updates are dynamically applied to the running application. This applies both to applications that are deployed through configuration entries, and those deployed from the “dropins” directory. You can change these default behaviors by setting the **config** and **applicationMonitor** elements in the `server.xml` configuration file. You can use a text editor to do this, or you can use the developer tools and select **Configuration Admin Service** or **Application Monitor** in the server configuration design view.

See also the descriptions of the **config** and **applicationMonitor** elements in .

The default settings for application monitoring are as follows:

```
<applicationMonitor updateTrigger="polled" pollingRate="500ms"
  dropins="dropins" dropinsEnabled="true"/>
```

The default settings for configuration monitoring are as follows:

```
<config updateTrigger="polled" monitorInterval="500ms"/>
```

#### Notes:

- The **updateTrigger** property has three possible values:
  - polled** The runtime environment scans the `server.xml` file for changes using the timing interval specified by the **monitorInterval** property.

## **mbean**

The runtime environment only looks for updates when prompted to do so through a call to an MBean. This is the mode that is used by the developer tools to update the `server.xml` file, unless you override it.

## **disabled**

The updates are not dynamically applied.

- When you specify the **pollingRate** property or the **monitorInterval** property, you include the unit of time after the number:
  - ms (milliseconds)
  - s (seconds)
  - m (minutes)
  - h (hours)
- The **dropins** property specifies the name of the directory used as the “dropins” directory.
- The **dropinsEnabled** property is a boolean property that determines whether the applications in the “dropins” directory are deployed.

## **Procedure**

- Configure dynamic changes to the server configuration.

Changes to the `server.xml` file, or any files it includes, are detected by the runtime environment and applied to the active configuration. You can disable this behavior by setting the **config** element in the `server.xml` file:

```
<config updateTrigger="disabled"/>
```

You can also control dynamic updates to the server configuration through a provided mbean by setting the **config** element in the `server.xml` file:

```
<config updateTrigger="mbean"/>
```

You can then use the `FileNotificationMbean` to notify the server which configuration file or files you want to be dynamically reprocessed.

- Configure dynamic addition and removal of applications.

As described in Chapter 10, “Deploying applications in Liberty,” on page 2139, applications can be dynamically added to and removed from the server runtime environment through two mechanisms:

- By adding or removing application entries in the `server.xml` file.

If you disable dynamic changes to the server configuration as described in the previous step, then adding or removing application entries has no effect on a running server. Your changes are only applied at the next server restart. The changes are picked up immediately, if you update application entries using the developer tools.

- By moving application files into and out of the “dropins” directory.

This behavior can be controlled by setting the **applicationMonitor** element in the `server.xml` file. For example, to disable dynamic installation of applications from the “dropins” location, create an entry as follows:

```
<applicationMonitor dropinsEnabled="false"/>
```

- Configure dynamic updates to installed applications.

By default, if you add, remove or modify any files within a deployed application, or you replace the whole application with an updated version, the previous version is automatically stopped and the new version is started. This process applies for any deployed application, whether the application is in the “dropins” directory or at a location defined in the `server.xml` file. You can control this behavior by setting the **applicationMonitor** element in the `server.xml` file. For example, to disable dynamic update of all applications, create an entry as follows:

```
<applicationMonitor updateTrigger="disabled"/>
```

- Configure the name and location of the “dropins” directory.

By default, the “dropins” directory is `${server.config.dir}/dropins`. You can change this by setting the **applicationMonitor** element in the `server.xml` file. For the location, you can use any known variable, or a property in the `bootstrap.properties` file, or an absolute path, or a path relative to the server directory. For example, both the following settings point to the same location:

```
<applicationMonitor dropins="${server.config.dir}/applications" />
<applicationMonitor dropins="applications" />
```

**Restriction:** For web service applications, if the service client and service provider are not in the same application and the WSDL file in the service provider application is changed, you need to restart the web service client application manually to avoid the WSDL definition cache issue.

## Configuring class loaders and libraries for Java EE applications

By default, each application can access a set of provided APIs and its own internal classes and libraries. You can override the default settings, and configure class loading for each application.

### About this task

Each Java EE application has its own class loader in a running Liberty server. Liberty assumes some default settings for all Java EE applications, so that they can access the supported specification APIs (for example the servlet APIs if the servlet feature is enabled), and the IBM APIs. By default, each application can access these provided APIs and access its own internal classes and libraries. If you have to override the default settings and configure class loading for your application, complete one or more of the following tasks.

**Note:** If you use configuration to override the default settings, you cannot deploy the application by dropping it into the “dropins” directory.

### Procedure

- “Using a Java library with a Java EE application”
- “Sharing a library across multiple Java EE applications” on page 1597
- “Accessing third-party APIs from a Java EE application” on page 1598
- “Removing access to third-party APIs for a Java EE application” on page 1599
- “Overriding a provided API with an alternative version” on page 1600
- “Providing global libraries for all Java EE applications” on page 1598

### Using a Java library with a Java EE application

One way of using Java libraries with an application is to include them in the application itself. This might not always be desirable or appropriate, especially if the application is already packaged and does not include the library.

### About this task

In the following example, a library called Alexandria consists of two files:

- `alexandria-scrolls.jar` and
- `commons-lang.jar`

An application called Scholar, running on a server called Academy, needs access to this library.

### Procedure

1. Create a `mylib/Alexandria` directory in the `servers/Academy` directory under the `${WLP_USER_DIR}` directory.  
For example: `wlp/usr/servers/Academy/mylib/Alexandria`.
2. Copy the `alexandria-scrolls.jar` and `commons-lang.jar` files into the new folder.

3. Configure class loading for the application, so that the Alexandria library is loaded.

In the `server.xml` file, or an included file, add the following code:

```
<application id="scholar" name="Scholar" type="ear" location="scholar.ear">
  <classloader>
    <privateLibrary>
      <fileset dir="{server.config.dir}/mylib/Alexandria" includes="*.jar" scanInterval="5s" />
    </privateLibrary>
  </classloader>
</application>
```

**Note:** The `<privateLibrary>` element can also take a `filesetRef` attribute with a comma-separated list of `<fileset>` element IDs.

## Sharing a library across multiple Java EE applications

Libraries can be shared across multiple Java EE applications. All the applications can use the same classes at run time, or each application can use its own separate copy of those classes loaded from the same location.

### About this task

In the following example, a library called Alexandria consists of two files:

- `alexandria-scrolls.jar` and
- `commons-lang.jar`

An application called Scholar and an application called Student are running on a server called Academy, and both need access to this library.

### Procedure

1. Create a `mylib/Alexandria` directory in the `servers/Academy` directory under the `{WLP_USER_DIR}` directory.

For example: `wlp/usr/servers/Academy/mylib/Alexandria`.

2. Copy the `alexandria-scrolls.jar` and `commons-lang.jar` files into the new folder.
3. Configure class loading for the application, so that the Alexandria library is loaded.

In the `server.xml` file, or an included file, define the library by adding the following code:

```
<library id="Alexandria">
  <fileset dir="{server.config.dir}/mylib/Alexandria" includes="*.jar" scanInterval="5s" />
</library>
```

**Note:** The `<library>` element can also take a `filesetRef` attribute with a comma-separated list of `<fileset>` element IDs.

4. Reference the library from the applications, so that both these applications share a single copy of the library.

In the `server.xml` file, or an included file, add the following code:

```
<application id="scholar" name="Scholar" type="ear" location="scholar.ear">
  <classloader commonLibraryRef="Alexandria" />
</application>

<application id="student" name="Student" type="ear" location="student.ear">
  <classloader commonLibraryRef="Alexandria" />
</application>
```

**Note:** The `<commonLibraryRef>` element can take a comma-separated list of library IDs.

5. Optional: Configure another application to have its own set of classes loaded from the same JAR files. For example, if another application called Spy needs its own copy of the classes, the same physical files on disk can be used. In the `server.xml` file, or an included file, add the following code:

```
<application id="spy" name="Spy" type="war" location="spy.war">
  <classloader privateLibraryRef="Alexandria" />
</application>
```

**Note:** The `<privateLibraryRef>` element can take a comma-separated list of library IDs.

## Providing global libraries for all Java EE applications

You can provide global libraries that can be used by any Java EE application. You do this by putting the JAR files for those libraries in a global library directory, then specifying use of global libraries in the class loader configuration for each application. However, the global libraries cannot be used by other applications, for example, by OSGi applications.

### About this task

Under the user directory specified by using the environment variable `WLP_USER_DIR`, there are the following locations in which you can place global libraries:

- `${shared.config.dir}/lib/global`
- `${server.config.dir}/lib/global`

If there are files present in these locations at the time an application is started, and that application does not have a `<classloader>` element configured, the application uses these libraries. If a class loader configuration is present, these libraries are not used unless the global library is explicitly referenced.

**Attention:** If you use global libraries, you are advised also to configure a `<classloader>` element for every application. The servlet specification requires applications to share the global library class loader in their class loader parent chain. This breaks the separation of class loaders for each application that is otherwise possible. So, applications are more likely to have long-lasting effects on classes loaded in Liberty and on each other, and class space consistency issues are more likely to arise between applications, especially as features are added and removed from a running server. None of these considerations apply for applications that specify a `<classloader>` element in their configuration, because they maintain this separation.

### Example

In the following example, an application called `Scholar` is configured to use a common library called `Alexandria`, and also to use the global library.

In the `server.xml` file, or an included file, enable the global library for an application by adding the following code:

```
<application id="" name="Scholar" type="ear" location="scholar.ear">
  <classloader apiTypeVisibility="spec" commonLibraryRef="Alexandria, global" />
</application>
```

The settings for the global library can also be configured explicitly, as a library element with the special ID `global`. For example:

```
<library id="global">
  <fileset dir="/path/to/folder" includes="*.jar" />
</library>
```

## Accessing third-party APIs from a Java EE application

By default, Java EE applications do not have access to the third-party APIs available in Liberty. To enable this access, the application must be configured in the `server.xml` file, or an included file.

## About this task

In the following example, an application that is called Scholar needs access to the third-party APIs that are available in Liberty.

The application also uses a common library called Alexandria. This library is located in the `${server.config.dir}/mylib/Alexandria` directory.

**Avoid trouble:** Third party APIs might not remain compatible after an upgrade. For more information, see “Liberty externals support” on page 19.

## Procedure

1. Configure class loading for the application, so that the application can access the third-party APIs.

The default value for the `apiTypeVisibility` attribute of the `classloader` element is `spec,ibm-api,api`. Where `spec` represents public specification APIs available for both compile and run time, `ibm-api` represents APIs available in Liberty, and `api` represents public APIs available for both compile and run time. Including `third-party` in the `apiTypeVisibility` attribute of the `classloader` element makes third party APIs available.

In the `server.xml` file, or an included file, configure the API type visibility by adding the following code:

```
<application id="scholar" name="Scholar" type="ear" location="scholar.ear">
  <classloader apiTypeVisibility="spec, ibm-api, third-party" commonLibraryRef="Alexandria" />
</application>
```

2. Optional: If the application uses any common libraries, set those libraries to use the same API type visibility setting.

In the `server.xml` file, or an included file, add the following code:

```
<library id="Alexandria" apiTypeVisibility="spec, ibm-api, third-party">
  <fileset dir="${server.config.dir}/mylib/Alexandria" includes="*.jar" scanInterval="5s" />
</library>
```

## Removing access to third-party APIs for a Java EE application

By default, Java EE applications do not have access to the third-party APIs available in Liberty. You can also remove access explicitly in the `server.xml` file, or an included file.

## About this task

In the following example, an application called Scholar has previously been configured to access third-party APIs, as described in “Accessing third-party APIs from a Java EE application” on page 1598. You want to remove this access, and to make it explicit in the configuration that the application now uses the default access setting.

The application also uses a common library called Alexandria. This library is in the `${server.config.dir}/mylib/Alexandria` directory.

## Procedure

1. Configure class loading for the application, to show that the application can no longer access the third-party APIs.

In the `server.xml` file, or an included file, remove `third-party` from the set of values included for the `apiTypeVisibility` attribute:

```
<application id="scholar" name="Scholar" type="ear" location="scholar.ear">
  <classloader apiTypeVisibility="spec, ibm-api" commonLibraryRef="Alexandria" />
</application>
```

2. Optional: If the application uses any common libraries, set those libraries to use the same API type visibility setting.

In the `server.xml` file, or an included file, add the following code:

```
<library id="Alexandria" apiTypeVisibility="spec, ibm-api">
  <fileset dir="${server.config.dir}/mylib/Alexandria" includes="*.jar" scanInterval="5s" />
</library>
```

## Overriding a provided API with an alternative version

If an application provides (or uses a library that provides) classes that are also available in Liberty, by default the classes from Liberty are used. To change this so that the application uses the alternative versions of these classes, the application must be configured in the `server.xml` file, or an included file.

### About this task

If a web application includes classes that are also present in the server runtime environment, you might want to control which copy of each of those classes is used by the application. For example, if different versions of the classes are present in both the application and the server runtime environment, you must ensure that the version packaged in the application is used.

By default, classes from the Liberty runtime environment are used by all Java EE applications. You can override this behavior by using the class loader configuration **delegation** attribute. This configuration is specific to a particular application, or to a shared library that can be selected for use by an application.

### Example

In the following example, an application called `Scholar` needs to use classes that it provides (or that are provided in a library that it uses), rather than using the copies of the classes that are available in Liberty.

- When the classes are packaged within the application, override the default `parentFirst` delegation behavior with a `classloader` element in the `server.xml` configuration file or a file that it includes:

```
<application id="" name="Scholar" type="ear" location="scholar.ear">
  <classloader delegation="parentLast" />
</application>
```

This tells the application class loader to look at the Liberty classes only after looking in the application and its associated libraries for a class.

- When the classes are packaged in a shared library, add the **delegation** attribute to the `classloader` element that configures the use of the shared library as follows:

```
<application id="" name="Scholar" type="ear" location="scholar.ear">
  <classloader delegation="parentLast" commonLibraryRef="mySharedLib"/>
</application>
```

```
<library id="mySharedLib">
  <fileset dir="${server.config.dir}/myLib" includes="*.jar" />
</library>
```

You can also use the **privateLibraryRef** attribute for private libraries in an application. See “Sharing a library across multiple Java EE applications” on page 1597.

## Configuring libraries for OSGi applications

8.5.5.6

Each OSGi application can access a set of provided APIs and its own internal classes. Shared libraries can also be configured to provide access to extra packages from shared libraries.

### About this task

Each OSGi application has its own set of OSGi bundles in a running Liberty server. Each OSGi bundle specifies the packages that it needs and the packages it provides for use by other OSGi bundles. Bundles

within an OSGi application can access any packages that are provided by other bundles within the same OSGi application. Additionally, OSGi bundles within an OSGi application can access API packages provided by the Liberty server. Shared libraries can also be used to provide API packages for use by OSGi applications.

Libraries can be shared across multiple OSGi applications. All the applications, including Java EE applications, can use the same classes at runtime that are provided by shared libraries.

## Procedure

1. Create a `mylib/osgi` directory in the `servers/defaultServer` directory under `${WLP_USER_DIR}` directory. For example: `wlp/usr/servers/defaultServer/mylib/osgi`.
2. Copy the `osgi-lib.jar` and `commons-lang.jar` files into the new folder.
3. Configure the shared library for the application so that the library is loaded. In the `server.xml` file, or an included file, define the library by adding the following code:

```
<library id="mylib">
  <fileset dir="${server.config.dir}/mylib/osgi" includes="*.jar" scanInterval="5s">
</library>
```

**Note:** The `library` element can also take a `filesetRef` attribute with a comma-separated list of `fileset` element IDs.

4. Reference the library as an OSGi library so that OSGi applications can access the packages provided by the library and share a single copy of the library. In the `server.xml` file, or an included file, add the following code:

```
<osgiLibrary libraryRef="myLib"/>
```

5. Optional: Configure the list of packages to make them available for access from OSGi applications. Packages that are contained in the shared library can be accessed by OSGi applications when the library is configured by using the `osgiLibrary` element. Packages can also be listed to give more control over what packages are accessible by OSGi applications. The package syntax uses the OSGi `Export-Package` header syntax to define each package. To list the packages in the `server.xml` file, or an included file, add the following code:

```
<osgiLibrary libraryRef="myLib">
  <package>org.example.osgi.lib.pkg1; version=1.0</package>
  <package>org.example.osgi.lib.pkg2; version=1.1</package>
</osgiLibrary>
```

**Note:** When no package elements are used, the library is scanned to find the packages that the library provides. Each package that is discovered gets the default version of 0.0.0.

## Configuring JPA for Liberty

8.5.5.6

### About this task

Java Persistence API (JPA) 2.0 for WebSphere Application Server is built on the Apache OpenJPA 2.2.x open source project.

Apache OpenJPA is a compliant implementation of the JPA 1.0 and 2.0 specifications. Using OpenJPA as a base implementation, WebSphere Application Server employs extensions to provide more features and utilities for WebSphere Application Server customers. Because JPA for WebSphere Application Server is built from OpenJPA, all OpenJPA function, extensions, and configurations are unaffected by the WebSphere Application Server extensions. You do not need to make changes to OpenJPA applications to use these applications in WebSphere Application Server.

Java Persistence API (JPA) 2.1 for WebSphere Application Server is built on the EclipseLink open source project. EclipseLink is the reference implementation for all version of the JPA specification. The provider

of JPA for this product is `org.eclipse.persistence.jpa.PersistenceProvider`.

## Configuring JPA logging

8.5.5.6

Logging supports viewing, tracing, and troubleshooting the runtime behavior of an application. Each of the JPA features provides different levels of logging for you to specify how detailed you want the logging to be.

### About this task

When using either the `jpa-2.0` or `jpa-2.1` features, you can configure logging to aid in troubleshooting. Become familiar with the logging capabilities of these two features.

#### **jpa-2.0**

There are many supported `jpa-2.0` trace specifications that can be configured through the Liberty configuration. These trace strings can be used in conjunction with any other trace specifications.

##### Container-managed JPA applications

- `JPA=all`  
Enables all JPA container trace and all OpenJPA tracing
- `openjpa=all`  
Enables all OpenJPA tracing
- OpenJPA specific log channels

```
openjpa.jdbc.SQL=all
```

```
<server>
```

```
...
```

```
<logging traceSpecification="openjpa.jdbc.SQL=all"  
  traceFileName="trace.log"  
  maxFileSize="20"  
  maxFiles="10"  
  traceFormat="BASIC" />  
</server>
```

##### Application managed JPA applications

When running a JPA application that is application managed, logging and tracing is controlled by the OpenJPA runtime. All JPA tracing and logging must be configured through OpenJPA persistence properties.

```
<persistence version="2.0">  
<persistence-unit>  
  <properties>  
    <property name="openjpa.Log" value="openjpa.jdbc.SQL=trace"/>  
  </properties>  
</persistence-unit>  
</persistence>
```

##### Notable OpenJPA logging persistence properties

`openjpa.ConnectionFactoryProperties=PrintParameters=true`-- If true, SQL bind parameters are included in exceptions and logs.

#### **jpa-2.1**

When the `jpa-2.1` feature is enabled, all JPA logging and tracing is routed through the Liberty loggers.

##### Supported trace strings

- `JPA=all`  
Enables JPA container trace and all EclipseLink categories
- `eclipselink=all`

Enables all EclipseLink trace

- EclipseLink specific log categories
  - sql, transaction, event, connection, query, cache, propagation, sequencing, ejb, dms, metadata, weaver, properties, server
  - ie: eclipselink.sql=All -- Enables EclipseLink SQL trace

```
<server>
...
<logging traceSpecification="eclipselink.sql=all"
  traceFileName="trace.log"
  maxFileSize="20"
  maxFiles="10"
  traceFormat="BASIC" />
</server>
```

### Notable EclipseLink logging persistence properties

eclipselink.logging.parameters -- If true, SQL bind parameters are included in exceptions and logs.

### Procedure

In the persistence unit definition in the persistence.xml file, specify the logging level depending on the desired level of logging details that you want. Specify the eclipselink.logging.level property where the value is the logging level. For the list of logging levels available, refer to the EclipseLink logging wiki page. The following example will turn on all logging that is available.

```
<persistence-unit name="pu">
  <properties>
    <property name="eclipselink.logging.level" value="ALL"/>
  ...
  </properties>
</persistence-unit>
```

## Configuring the JPA 2.1 schema generator

8.5.5.6

In the jpa-2.0 feature, which is built on OpenJPA, you can generate data definition language (DDL) or interact directly with the database to define table schemas based on the JPA entity definition by using the SchemaMapper tool. In the jpa-2.1 feature, which is built on EclipseLink, you can use the new Schema Generator feature added to the JPA 2.1 specification, which has similar functions to the OpenJPA SchemaMapper.

### About this task

If you need functions similar to the OpenJPA SchemaMapper, you can configure the Schema Generator feature that is in the JPA 2.1 specification.

### Procedure

1. In the persistence unit definition, within the persistence.xml file, specify the database action property with the possible values of: none, create, drop, drop-and-create. Each value corresponds to the action that is taken against the database. The following example causes the tables that correspond to the entities specified in the persistence unit to be dropped and new tables are created in their place.

```
<persistence-unit name="pu">
  <properties>
    <property name="javax.persistence.schema-generation.database.action"
  value="drop-and-create" />
  ...
  </properties>
</persistence-unit>
```

2. Specify the script action property with the possible values of: none, create, drop, drop-and-create. If any value other than none is specified, you must specify a target property as well. This means that if the script action is create, which generates the create statements for the entity definition, you must specify a corresponding create target property with a target file where the statements are written to.

```
<persistence-unit name="pu">
  <properties>
    <property name="javax.persistence.schema-generation.scripts.action"
value="drop-and-create" />
    <property name="javax.persistence.schema-generation.scripts.create-target"
value="createTargetFile.ddl"/>
    <property name="javax.persistence.schema-generation.scripts.drop-target"
value="sampleDrop.ddl"/>
  ...
  </properties>
</persistence-unit>
```

## Disabling the EclipseLink shared object cache

8.5.5.6

The EclipseLink shared object cache contains a subset of all objects that are read and persisted for the persistence unit. The EclipseLink shared cache differs from the local EntityManager/L1/persistence context cache. The shared cache exists during the persistence unit and is shared by all EntityManagers and users of the persistence unit.

### About this task

If you are migrating an existing application or running an environment where your application spans multiple Java Virtual Machines (JVMs), you can disable the EclipseLink shared object cache.

Choose one of the following ways to disable the EclipseLink shared object cache.

### Procedure

- Set the `<shared-cache-mode>NONE</shared-cache-mode>` property in the `persistence.xml` file.

```
<persistence-unit name="pu">
  <shared-cache-mode>NONE</shared-cache-mode>
  <properties>
  ...
  </properties>
</persistence-unit>
```

- Set the `eclipselink.cache.shared.default` property to `false` in the persistence unit definition that is found in the `persistence.xml` file.

```
<persistence-unit name="pu">
  <properties>
    <property name="eclipselink.cache.shared.default" value="false" />
  ...
  </properties>
</persistence-unit>
```

## Configuring a web server plug-in for Liberty

You can configure a web server plug-in to receive an HTTP request for dynamic resources. You can forward the request to the Liberty server, which provides high-availability and workload balancing through the web server plug-in.

### Before you begin

1. Install a supported web server, such as the IBM HTTP Server that is included with IBM WebSphere Application Server. See [Installing IBM HTTP server](#) for more information. The web server that is provided with IBM i is already installed with product 5761-DG1 for IBM i V6R1, or 5770-DG1 for IBM i V7R1. The IBM i web server is referred to as the IBM HTTP Server for IBM i. The HTTP Server that

is provided with WebSphere Application Server does not run on IBM i and is included for z/OS, V7 and V8.0. To download the V8.5 HTTP server, see IBM Ported Tools for z/OS .

2. Install the web server plug-ins and the WebSphere Customization Toolbox (WCT). To install the web server plug-in, see Installing and configuring web server plug-ins .

**IBM i** For IBM i, see Installing and configuring web server plug-ins .

**z/OS** For IBM z/OS, see Installing Web Server Plug-ins for IBM WebSphere Application Server for z/OS .To install the WCT, see Installing and using the WebSphere Customization Toolbox.

**IBM i** **z/OS** For IBM i and z/OS, install the WCT on your workstation. You do not need to install any of the WCT tools. The Java SDK installed with the WCT is used to run the JConsole Java utility in a later step.

## About this task

A web server plug-in is used to forward HTTP requests from a supported web server to one or more application servers. The plug-in checks the request against configuration data in the `plugin-cfg.xml` file. The configuration data maps the URI for the HTTP request to the host name of an application server. The web server plug-in then uses this information to forward the request to the application server.

The procedure applies to Liberty servers not in a collective.

## Procedure

1. Configure the web server plug-in for your chosen web server by using the WCT.
  - When prompted in WCT, choose the **remote** scenario and specify the host name that Liberty is accessible on.
  - Do not copy or run the generated `configureWebserver` script. This script is not required with Liberty.

**z/OS** This step is not necessary for z/OS platforms.

2. **IBM i** **z/OS** Configure your HTTP server to use the `plugin-cfg.xml` file.

Find the location of your current `plugin-cfg.xml` by finding the value that is specified for the `WebSpherePluginConfig` directive at the end of the configuration file of the HTTP server. For example, `<IHS_ROOT>/conf/httpd.conf`.

Enable the plug-in within the `httpd.conf` file of the web server by using the `LoadModule` phrase, and specify the location of `plugin-cfg.xml` file by using the `WebSpherePluginConfig` phrase. For example:

- On Windows systems: **Windows**

```
LoadModule was_ap22_module "path/to/mod_was_ap22_http.dll"  
WebSpherePluginConfig "C:\Program Files\IBM\HTTPServer\conf\plugin-cfg.xml"
```

- On other distributed systems: **AIX** **Linux** **UNIX** **HP-UX** **Solaris**

```
LoadModule was_ap22_module "path/to/mod_was_ap22_http.so"  
WebSpherePluginConfig "/opt/IBM/HTTPServer/conf/plugin-cfg.xml"
```

**IBM i** **z/OS** For IBM i and z/OS, see [http://www14.software.ibm.com/webapp/wsbroker/redirect?version=phil&product=was-nd-mp&topic=tins\\_manualWebIHS80](http://www14.software.ibm.com/webapp/wsbroker/redirect?version=phil&product=was-nd-mp&topic=tins_manualWebIHS80) for instructions about enabling the plug-in within the `httpd.conf` file.

3. Optional: If you want the web server plug-in to forward HTTP requests to more than one Liberty server, repeat the previous steps for each additional server. Make sure that you consolidate all the plug-in configurations into one `plugin-cfg.xml` file.
  - You can use a `pluginCfgMerge` utility in the traditional server to merge multiple `plugin-cfg.xml` files. See Configuring simple load balancing across multiple application server profiles .
  - You can use a Plugin Merge command-line tool available on GitHub to merge individual configuration files into a single `merged-plugin-cfg.xml` file.

- If you are using the job manager to merge multiple `plugin-cfg.xml` files, see [Generating a merged plug-in configuration for Liberty servers using the job manager](#).

## Generating a merged plug-in configuration for Liberty servers

### 8.5.5.0

You can call the `ClusterManager` MBean `generateClusterPluginConfig` operation to create a single, merged `plugin-cfg.xml` file that instructs a web server plug-in to redirect requests to multiple application servers residing on multiple hosts.

### About this task

The operation first generates server-specific `plugin-cfg.xml` files on each started cluster member. The operation then merges the server-specific `plugin-cfg.xml` files into one `plugin-cfg.xml` file on the cluster manager.

This operation works only if the cluster has at least two started cluster members. The path to the merged `plugin-cfg.xml` file on the cluster manager is returned to the client. Therefore, it can be downloaded using the `fileTransfer` MBean.

The merged `plugin-cfg.xml` file name is `<clusterName>-plugin-cfg.xml`. It is saved in the following directory on the cluster manager by default:

```

${server.output.dir}/pluginConfig

```

This directory can be changed by providing the `clusterPluginConfig` element in the `server.xml` file:

```

<clusterPluginConfig>
  <outputDir>new output directory</outputDir>
</clusterPluginConfig>

```

**Note:** Make sure that the new output directory is writable and accessible by the `fileTransfer` MBean. Refer to the `fileTransfer` MBean documentation for details.

### Example:

```

// call the generateClusterPluginConfig operation on the ClusterManager MBean to generate
// a merged plugin-cfg.xml file for all started cluster members.
String clusterName = "myCluster";
ObjectName rmObjectName = new ObjectName("WebSphere:feature=collectiveController,type=ClusterManager,name=ClusterManager");

// rcObj contains the absolute path to the merged plugin-cfg.xml file.
Object rcObj = connection.invoke(rmObjectName, "generateClusterPluginConfig",
    new Object[] { clusterName },
    new String[] { "java.lang.String" });

// invoke the downloadFile operation on fileTransfer MBean to download the merged plugin-cfg.xml to the client.
String sourceFilePath = (String) rcObj;
String targetFilePath = "<my target directory>";
ObjectName objectName = new ObjectName("WebSphere:feature=restConnector,type=FileTransfer,name=FileTransfer");

connection.invoke(objectName, "downloadFile",
    new String[] { sourceFilePath, targetFilePath },
    new String[] { "java.lang.String", "java.lang.String" });

```

Refer to the `ClusterManager` MBean documentation for additional information on cluster management.

## Generating the plugin-cfg.xml file

This information can be used to generate the `plugin-cfg.xml` file for the web server, which is used to forward HTTP requests from a supported web server to one or more application servers. The plug-in takes a request and checks the request against configuration data in the `plugin-cfg.xml` file.

## Before you begin

If an application programmatically modifies the session cookie configuration by using Servlet 3.0 APIs, then the application must be initialized before you generate the `plugin-cfg.xml` file. Otherwise, the **AffinityCookie** attribute that is defined for that application might be wrong. To avoid this problem, you can set **deferServletLoad** to false, start the server, generate the plug-in, and then remove the **deferServletLoad** attribute.

## About this task

A web server plug-in is used to forward HTTP requests from a supported web server to one or more application servers. The plug-in takes a request and checks the request against configuration data in the `plugin-cfg.xml` file. The configuration data maps the URI for the HTTP request to the host name of an application server. The web server plug-in then uses this information to forward the request to the application server.

## Procedure

1. Start the server that hosts your applications, and ensure that the `localConnector-1.0` feature for IBM i and z/OS platforms, or the `restConnector-1.0` feature if you are configuring a plug-in for IBM i or z/OS, and any other required features are included in the server configuration.

In the `pluginConfiguration` element of the server configuration file, you can specify the **webserverPort** and **webserverSecurePort** attributes to forward requests from the web server. By default, the value of **webserverPort** is 80 and the value of **webserverSecurePort** is 443. However, you might want to change these settings. For example, for Linux and similar platforms, if you are a non-root user, you must use port numbers greater than 1024.

For all configurable attributes of the `pluginConfiguration` element, see “Java Servlets 3.1” on page 917.

Here is an example of a `server.xml` server configuration file:

```
<server description="new server">
  <featureManager>
    <feature>localConnector-1.0</feature>
    <feature>jsp-2.2</feature>
  </featureManager>

  <keyStore id="defaultKeyStore" password="{xor}PGY6bW4w0yw+" />

  <httpEndpoint id="defaultHttpEndpoint"
    host="*"
    httpPort="9080">
    <tcpOptions soReuseAddr="true" />
  </httpEndpoint>

  <pluginConfiguration webserverPort="80"
    webserverSecurePort="443"
    sslKeyringLocation="path/to/sslkeyring"
    sslStashfileLocation="path/to/stashfile"
    sslCertlabel="definedbyuser"/>

  <application type="war" id="myapp" name="myapp" location="${server.config.dir}/apps/myapp.war" />
  <application type="war" id="snoop" name="snoop" location="${server.config.dir}/apps/snoop.war" />
</server>
```

**IBM i** **z/OS** For IBM i and z/OS, include the `restConnector-1.0` feature instead of the `localConnector-1.0` feature. For details, see [Configuring secure JMX connection to Liberty](#).

**IBM i** **z/OS** Here is an example of a `server.xml` server configuration file for IBM i and z/OS:

```
<server description="new server">
<!-- Enable features -->
```

```

<featureManager>
  <feature>jsp-2.2</feature>
  <feature>restConnector-1.0</feature>
</featureManager>

<keyStore id="defaultKeyStore" password="{xor}PGY6bW4w0yw+" />

<httpEndpoint id="defaultHttpEndpoint"
  host="*"
  httpPort="9080"
  httpsPort="9443">
  <tcpOptions soReuseAddr="true" />
</httpEndpoint>

<quickStartSecurity userName="testuser"
  userPassword="security" />

<pluginConfiguration webserverPort="80"
  webserverSecurePort="443"
  sslKeyringLocation="path/to/sslkeyring"
  sslStashfileLocation="path/to/stashfile"
  sslCertlabel="definedbyuser"/>

<application type="war" id="myapp" name="myapp" location="${server.config.dir}/apps/myapp.war" />
<application type="war" id="snoop" name="snoop" location="${server.config.dir}/apps/snoop.war" />
</server>

```

**Note:**

- If you configure the web server plug-in to use SSL, you must enable the ssl-1.0 Liberty feature of Liberty.
  - If the web server is using the default ports, you do not have to include the pluginConfiguration element in the server.xml file.
  - The keystore that is used by the web server plug-in must be a CMS keystore, which can be created by using the Key Management (iKeyman) utility. You cannot use the JKS keystore that is created by Liberty or traditional for the web server plug-in, though you must exchange signer certificates between the web server plug-in keystore and the Liberty keystore.
  - To configure the location of the plug-in log file, add the following code snippet to the server.xml file within the pluginConfiguration element:
 

```
logDirLocation="/path/to/log/file/"
```
2. Generate the plugin-cfg.xml file for your Liberty server and applications by calling the WebSphere:name=com.ibm.ws.jmx.mbeans.generatePluginConfig MBean.
- a. Using the same Java SDK as the server, run the **jconsole** Java utility in a command window. For example, run the following command:
- ```
c:\java\bin\jconsole
```

The server process is listed in the choices that are waiting for connection.

**IBM i** **z/OS** For IBM i and z/OS, run the jconsole Java utility from a command window by using the Java SDK installed with the WCT on your workstation. For example, complete the following steps:

- 1) Create directory C:\restClient on your workstation.
- 2) Copy \${wlp.install.dir}/clients/restConnector.jar to the C:\restClient directory on your workstation.
- 3) Copy \${server.output.dir}/resources/security/key.jks to the C:\restClient directory on your workstation.
- 4) In a command window, type SET JAVA\_HOME=wct\_root\java.

**Note:** Ensure that you temporarily modify `wct_root\java\jre\lib\security\java.security` by commenting out the two lines that set the SSL socket factories to the WebSphere Application Server SSL socket factories. This modification is documented in the Troubleshooting SSL section of the troubleshooting tips topic.

- 5) From the same command window, run the **jconsole** Java utility.

For example, run the following command:

```
"%JAVA_HOME%\bin\jconsole -J-Djava.class.path=%JAVA_HOME%\lib\jconsole.jar;%JAVA_HOME%\lib\tools.jar;
C:\restClient\restConnector.jar -J-Djavax.net.ssl.trustStore=C:\restClient\key.jks
-J-Djavax.net.ssl.trustStorePassword=Liberty -J-Djavax.net.ssl.trustStoreType=jks
```

You might also need the following parameter:

```
-J-Dcom.ibm.ws.jmx.connector.client.disableURLHostnameVerification=true
```

- b. Connect to your server then click the **MBeans** tab.  After the jConsole starts, select **Remote Process**, and enter the JMX service URL: `service:jmx:rest://<host>:<port>/IBMJMXConnectorREST`. The port number is the HTTPS port. You must also provide the user name and password.
- c. Locate the `com.ibm.ws.jmx.mbeans.generatePluginConfig` MBean under the **WebSphere** domain.
- d. Call the `generateDefaultPluginConfig` operation to generate the `plugin-cfg.xml` file, or call the `generatePluginConfig` operation to customize installation root directory and server name before you generate the `plugin-cfg.xml` file.

Here is an example of a `plugin-cfg.xml` file:

```
<?xml version="1.0" encoding="UTF-8"?>
<Config ASDisableNagle="false" AcceptAllContent="false" AppServerPortPreference="HostHeader"
  ChunkedResponse="false" FIPSEnable="false" IISDisableNagle="false"
  IISPluginPriority="High" IgnoreDNSFailures="false" RefreshInterval="60"
  ResponseChunkSize="64" SSLConsolidate="false" SSLPKCSDriver="REPLACE"
  SSLPKCSPassword="REPLACE" TrustedProxyEnable="false" VHostMatchingCompat="false">
  <Log LogLevel="Error" Name=".\\logs\defaultServer\http_plugin.log"/>
  <Property Name="ESIEnable" Value="true"/>
  <Property Name="ESIMaxCacheSize" Value="1024"/>
  <Property Name="ESIInvalidationMonitor" Value="false"/>
  <Property Name="ESIEnableToPassCookies" Value="false"/>
  <Property Name="PluginInstallRoot" Value="."/>
  <VirtualHostGroup Name="default_host">
    <VirtualHost Name="*:80"/>
    <VirtualHost Name="*:443"/>
    <VirtualHost Name="*:9080"/>
  </VirtualHostGroup>
  <ServerCluster CloneSeparatorChange="false" GetDWLMTTable="false" IgnoreAffinityRequests="true"
    LoadBalance="Round Robin" Name="defaultServer_default_node_Cluster"
    PostBufferSize="64" PostSizeLimit="-1" RemoveSpecialHeaders="true"
    RetryInterval="60">
    <Server CloneID="b564bdc7-2c27-4a4b-ad37-9213c66e60d1" ConnectTimeout="0"
      ExtendedHandshake="false" MaxConnections="-1" Name="default_node_defaultServer0"
      ServerIOTimeout="900" WaitForContinue="false">
      <Transport Hostname="somehost.example.com" Port="9080" Protocol="http"/>
    </Server>
    <PrimaryServers>
      <Server Name="default_node_defaultServer0"/>
    </PrimaryServers>
  </ServerCluster>
  <UriGroup Name="default_host_defaultServer_default_node_Cluster_URIs">
    <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/myapp/*"/>
    <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/snoop/*"/>
  </UriGroup>
  <Route ServerCluster="defaultServer_default_node_Cluster"
    UriGroup="default_host_defaultServer_default_node_Cluster_URIs"
    VirtualHostGroup="default_host"/>
</Config>
```

The plugin-cfg.xml file is generated in the `${server.output.dir}` directory.

**Note:**

- You can use the **jConsole** utility with Liberty. However, any issues with the utility itself must be reported to your Java SDK provider.
  - The management interface for the `WebSphere:name=com.ibm.ws.jmx.mbeans.generatePluginConfigMBean` is `com.ibm.websphere.webcontainer.GeneratePluginConfigMBean`.
3. Copy the plugin-cfg.xml file to the machine that hosts the web server. **IBM i** For IBM i, complete the following steps:
- a. Run the **manageprofiles** Qshell command to create an http profile. For example, `plugins_root/bin/manageprofiles -create -profileName http -templatePath http`.
  - b. Copy the plugin-cfg.xml file to the config directory of the http profile that was created in substep a, for example, `plugin_profile_root/config/plugin-cfg.xml`, and set the file permissions.
  - c. Run the following command from a system command line to change the file authorities to the required settings:  

```
CHGAUT USER(QEJBSVR QTMHHTTP QNOTES) OBJ('plugin_profile_root/config/plugin-cfg.xml') DTAAUT(*RWX)
```

## Configuring session persistence for Liberty

When session data must be maintained across a server restart or an unexpected server failure, you can configure Liberty to persist the session data to a database. This configuration allows multiple servers to share the same session data, and session data can be recovered in the event of a failover.

### About this task

To configure one or more servers in Liberty to persist session data to a database, complete the following steps.

### Procedure

1. Define a shared session management configuration that you can reuse among all of your servers. You must complete the following steps, as a minimum requirement:
  - a. Enable the `sessionDatabase-1.0` feature.
  - b. Define a data source:

```
<dataSource id="SessionDS" ... />
```
  - c. Refer to the data source from the session database configuration.

```
<httpSessionDatabase id="SessionDB" dataSourceRef="SessionDS" ... />
```
  - d. Refer to the persistent storage location from the session management configuration.

```
<httpSession storageRef="SessionDB" ... />
```

**Note:** **8.5.5.0** The `storageRef` attribute of the `httpSession` element and the `id` attribute of the `httpSessionDatabase` element are not mandatory. If the `sessionDatabase-1.0` feature is enabled and the `httpSessionDatabase` element references a valid data source, session persistence is enabled even if the `storageRef` attribute is not set.

See for details about the `httpSession` and `httpSessionDatabase` elements.

For example, you can create a file named `${shared.config.dir}/httpSessionPersistence.xml` as follows:

```
<server description="Demonstrates HTTP Session Persistence Configuration">
  <featureManager>
    <feature>sessionDatabase-1.0</feature>
    <feature>servlet-3.0</feature>
  </featureManager>
```

```

<httpEndpoint id="defaultHttpEndpoint" host="*" httpPort="${httpPort}">
  <tcpOptions soReuseAddr="true"/>
</httpEndpoint>

<fileset id="DerbyFiles" includes="*.jar" dir="${shared.resource.dir}/derby/client"/>
<library id="DerbyLib" filesetRef="DerbyFiles"/>
<jdbcDriver id="DerbyDriver" libraryRef="DerbyLib"/>
<dataSource id="SessionDS" jdbcDriverRef="DerbyDriver">
  <properties.derby.client user="user1" password="password1"
    databaseName="${shared.resource.dir}/databases/SessionDB"
    createDatabase="create"/>
</dataSource>

<httpSessionDatabase id="SessionDB" dataSourceRef="SessionDS"/>
<httpSession storageRef="SessionDB" cloneId="${cloneId}"/>

<application id="test" name="test" type="ear" location="${shared.app.dir}/test.ear"/>
</server>

```

**Note:** When multiple servers are configured to persist session data to the same database, those servers must share the same session management configuration. Any other configuration is not supported. For example, it is not possible for one server to use a multi-row schema while another server uses a single-row schema.

The HTTP server plugin uses the clone ID that is inserted into the response/request header to maintain session affinity between requests. While the clone ID is normally unchanging, in Liberty, the clone ID is generated when you start a server for the first time and it is regenerated if you start the server with the `--clean` option. For production use, manually assigning a clone ID will ensure that the ID is stable and that request affinity is correctly maintained. The clone ID must be unique for each server and can be 8 to 9 alphanumeric characters in length and is specified in step 3.

2. Include the shared session management configuration in each of your servers. For example, create two `server.xml` files for server instances named `s1` and `s2`, as follows:

```

• ${wlp.user.dir}/servers/s1/server.xml
• ${wlp.user.dir}/servers/s2/server.xml
<server description="Example Server">
  <include location="${shared.config.dir}/httpSessionPersistence.xml"/>
</server>

```

See “Using include elements in configuration files” on page 1588.

3. Specify unique variables in the `bootstrap.properties` file of each server.

```

• ${wlp.user.dir}/servers/s1/bootstrap.properties
  httpPort=9081
  cloneId=s1
• ${wlp.user.dir}/servers/s2/bootstrap.properties
  httpPort=9082
  cloneId=s2

```

4. Create a table for session persistence before you start the servers.

- If you want to change the default row size, table name, or table space name, see for details about the `httpSessionDatabase` element.

- **Distributed operating systems** No additional action is required if your server is installed on one of the distributed operating systems. The server automatically creates the table.

- **z/OS** If your server is installed on z/OS, you have to create the table manually. If your server is using z/OS DB2 for session persistence, you have to follow different steps to create the table manually.

- If your server is using DB2 for session persistence, you can increase the page size to optimize performance for writing large amounts of data to the database.
5. Synchronize the system clocks of all machines that host Liberty servers. If the system clocks are not synchronized, session invalidation can occur prematurely
  6. Optional: If required, integrate HTTP sessions and security in Liberty. By default, after a session is created and accessed within a protected resource with security enabled, only the originating owner of that session can access it. Session security (security integration) is enabled by default.
  7. Optional: If required, Install and configure the web server plug-in to route requests to each of the servers you configured. The session affinity is only maintained if your plug-in configuration specifies clone IDs that match the clone IDs defined in the server configuration.

## Configuring and deploying a basic JCA ResourceAdapter

8.5.5.2



You can configure and deploy a basic Java™ EE Connector Architecture (JCA) ConnectionFactory and Resource Adapter.

### About this task

You can install a resource adapter and configure instances of the resources it provides. This task uses an example resource adapter called ExampleRA.rar, which provides 3 types of resources: a connection factory and two types of administered objects.

### Procedure

1. Enable the JCA feature in your server.xml file. The server.xml file is found at [path\_to\_liberty\wlp\usr\servers\server\_name]

```
<server>
  <featureManager>
    <feature>jca-1.6</feature>
    <feature>servlet-3.0</feature>
  </featureManager>
</server>
```

2. Place the resource adapter RAR file (ExampleRA.rar) into the dropins folder of your server. If your server is running, you will see the following message in your console log indicating that the resource adapter has been installed:

```
[AUDIT ] J2CA7001I: Resource adapter ExampleRA installed in 1.306 seconds.
```

3. Inspect the deployment descriptor, annotations, and other documentation from the resource adapter to identify which types of resources the adapter provides and the configuration properties that each adapter accepts. The example resource adapter, ExampleRA.rar, has this information in the ra.xml deployment descriptor. The ra.xml file is found at [path\_to\_ExampleRA\ExampleRA\META-INF.] The deployment descriptor identifies 3 types of resources you can configure.

```
<connection-definition>
  <managedconnectionfactory-class>com.ibm.example.jca.adapter.ManagedConnectionFactoryImpl</managedconnectionfactory-class>
  <config-property>
    <config-property-name>tableName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
  </config-property>
  <connectionfactory-interface>javax.resource.cci.ConnectionFactory</connectionfactory-interface>
  ...
</connection-definition>

  <adminobject>
    <adminobject-interface>javax.resource.cci.ConnectionSpec</adminobject-interface>
    <adminobject-class>com.ibm.example.jca.adapter.ConnectionSpecImpl</adminobject-class>
    <config-property>
      <config-property-name>readOnly</config-property-name>
```

```

    <config-property-type>java.lang.Boolean</config-property-type>
    <config-property-value>>false</config-property-value>
  </config-property>
</adminobject>

<adminobject>
  <adminobject-interface>javax.resource.cci.InteractionSpec</adminobject-interface>
  <adminobject-class>com.ibm.example.jca.adapter.InteractionSpecImpl</adminobject-class>
  <config-property>
    <description>Function name. Supported values are: ADD, FIND, REMOVE</description>
    <config-property-name>functionName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
  </config-property>
</adminobject>

```

4. In the server.xml file, configure instances of the available resource types.

```

<server>
  <featureManager>
    <feature>jca-1.6</feature>
    <feature>servlet-3.0</feature>
  </featureManager>

  <connectionFactory jndiName="eis/conFactory">
    <properties.ExampleRA tableName="TABLE1"/>
  </connectionFactory>

  <adminObject jndiName="eis/conSpec">
    <properties.ExampleRA.ConnectionSpec/>
  </adminObject>

  <adminObject jndiName="eis/iSpec_ADD">
    <properties.ExampleRA.InteractionSpec functionName="ADD"/>
  </adminObject>

  <adminObject jndiName="eis/iSpec_FIND">
    <properties.ExampleRA.InteractionSpec functionName="FIND"/>
  </adminObject>

</server>

```

5. Use resource injection to access the resources in your servlet; for example:

```

@Resource(lookup = "eis/conFactory")
private ConnectionFactory conFactory;

@Resource(lookup = "eis/conSpec")
private ConnectionSpec conSpec;

@Resource(lookup = "eis/iSpec_ADD")
private InteractionSpec iSpec_ADD;

@Resource(lookup = "eis/iSpec_FIND")
private InteractionSpec iSpec_FIND;

...

MappedRecord input = conFactory.getRecordFactory().createMappedRecord("input");
input.put("city", "Rochester");
input.put("state", "Minnesota");
input.put("population", 106769);

Connection con = conFactory.getConnection(conSpec);
try {
  Interaction interaction = con.createInteraction();
  interaction.execute(iSpec_ADD, input);
}

```

```

        interaction.close();
    } finally {
        con.close();
    }
}

```

**Note:** You must enable the JNDI feature in the `server.xml` file if you want to look up the resources from the namespace rather than using injection.

## Overview of JCA configuration elements

8.5.5.2



The Java Platform, Enterprise Edition Connector Architecture (JCA) feature provides configuration elements to define instances of connection factories, administered objects, and activation specifications, and to associate these instances with an installed resource adapter. Each of the JCA configuration elements consists of two basic parts, a top-level element and a subelement, both of which are required for the configured instance.

A *top-level element* configures general capabilities that are provided by the Liberty server, such as JNDI name, connection management, and container authentication. A *subelement* ties the instance to an installed resource adapter and enables you to specify vendor-defined configuration properties.

Generic JCA pre-defined top-level configuration elements:

- `connectionFactory`
- `adminObject`
- `activationSpec`

If the JMS feature is enabled, there are also pre-defined generic configuration elements for JMS:

- `jmsConnectionFactory`
- `jmsQueueConnectionFactory`
- `jmsTopicConnectionFactory`
- `jmsDestination`
- `jmsQueue`
- `jmsTopic`
- `jmsActivationSpec`

Subelements are generated from the resource adapter deployment descriptor and annotations when your resource adapter is installed. You will not see any documentation of the available subelements in the static documentation for available server configuration elements.

Use the following rules to generate the names of the server configuration subelements:

- If a resource adapter provides exactly one interface within one of the listed categories, such as `connectionFactory` or `adminObject`, the subelement is: `properties.<rar_identifier>`
- If the interface name is unique without the package name, the subelement is: `properties.<rar_identifier>.<InterfaceName>`
- If the implementation name is unique without the package name, the subelement is: `properties.<rar_identifier>.<ImplementationName>`
- In other cases, the subelement name is `properties.<rar_identifier>.<fully.qualified.InterfaceName>` or `properties.<rar_identifier>.<fully.qualified.ImplementationName>`

The following examples illustrate the case where only one interface within each category is provided by a resource adapter with identifier `MyAdapter`:

```

<connectionFactory jndiName="eis/cf1" containerAuthDataRef="auth1">
  <properties.MyAdapter portNumber="1234" someVendorProperty="100"/>
</connectionFactory>

<connectionFactory jndiName="eis/cf2" containerAuthDataRef="auth2">
  <properties.MyAdapter portNumber="1234" someVendorProperty="200"/>
</connectionFactory>

<jmsConnectionFactory jndiName="jms/cf">
  <properties.MyAdapter serverName="localhost" anotherProperty="40"/>
</jmsConnectionFactory>

<jmsQueueConnectionFactory jndiName="jms/qcf">
  <properties.MyAdapter serverName="localhost" vendorProp1="1"/>
</jmsQueueConnectionFactory>

<jmsTopicConnectionFactory jndiName="jms/tcf">
  <properties.MyAdapter serverName="localhost" prop1="A" prop2="B"/>
</jmsTopicConnectionFactory>

<adminObject jndiName="eis/interactionSpec">
  <properties.MyAdapter functionName="find" executionTimeout="5000"/>
</adminObject>

<jmsDestination jndiName="jms/destination1">
  <properties.MyAdapter name="DEST1"/>
</jmsDestination>

<jmsQueue jndiName="jms/queue1">
  <properties.MyAdapter queueName="QUEUE1"/>
</jmsQueue>

<jmsTopic id="topic1" jndiName="jms/topic1">
  <properties.MyAdapter topicName="TOPIC1"/>
</jmsTopic>

<activationSpec id="app1/module1/MyMessageDrivenBean">
  <properties.MyAdapter prop1="a" prop2="b" prop3="c"/>
</activationSpec>

<jmsActivationSpec id="app1/module1/MyJMSMessageDrivenBean">
  <properties.MyAdapter destinationRef="topic1"/>
</jmsActivationSpec>

```

## Configuring resource adapters: 8.5.5.2

You can configure resource adapters that comply with the Java EE Connector Architecture (JCA) specification versions 1.6, 1.5, or 1.0.

### About this task

You can install and configure a resource adapter and the various connection factories, administered objects, and activation specifications as defined in the JCA specification.

### Procedure

1. Update the `server.xml` file to add the `jca-1.6` feature under the `featureManager` tag. The `server.xml` file is found at `[path_to_liberty\wlp\usr\servers\server_name]`

```

<featureManager>
  <feature>jca-1.6</feature>
</featureManager>

```

2. (Optional) Enable the following additional features based on the needs of your system:

- If your resource adapter provides JMS specification interfaces, enable the `jms-1.1` feature.

```
<feature>jms-1.1</feature>
```
- If you want to look up connection factories and administered objects from your application, enable the `jndi-1.0` feature.

```
<feature>jndi-1.0</feature>
```

- If your resource adapter provides activation specifications for message driven beans, enable the mdb-3.1 feature.  
`<feature>mdb-3.1</feature>`
  - If your resource adapter supports inbound security, enable the jcaInboundSecurity-1.0 feature.  
`<feature>jcaInboundSecurity-1.0</feature>`
  - If your resource adapter supports bean validation and you want your beans to be validated, you can enable the beanValidation-1.0 feature.  
`<feature>beanValidation-1.0</feature>`
3. Configure one or more resource adapters in the server. You can use one of the following methods to configure the resource adapter.
- Configure a standalone resource adapter by editing the `theserver.xml` file.  
`<resourceAdapter location="C:/adapters/MyAdapter.rar"/>`
  - Configure an embedded resource adapter by editing the `server.xml` file to install an application that embeds one or more resource adapter modules. The following example assumes that the `app1.ear` file contains one or more embedded RAR files:  
`<application location="C:/applications/app1.ear"/>`
  - Allow the server to automatically configure a standalone resource adapter by dropping the RAR file in the server drop-ins folder.  
`wlp/usr/servers/your-server-name/dropins/MyDropinAdapter.rar`
  - Allow the server to automatically configure an application containing one or more embedded resource adapters by dropping the EAR file in the server drop-ins folder. The following example assumes that the `app2.ear` file contains one or more embedded RAR files:  
`wlp/usr/servers/your-server-name/dropins/app2.ear`
4. Start the application server. After the server is started, messages such as the following are displayed in the `console.log` file:
- ```
[AUDIT ] J2CA7001I: Resource adapter MyAdapter installed in 0.495 seconds.
[AUDIT ] J2CA7001I: Resource adapter MyDropinAdapter installed in 0.311 seconds.
[AUDIT ] J2CA7001I: Resource adapter app1.MyEmbeddedAdapter installed in 0.247 seconds.
[AUDIT ] J2CA7001I: Resource adapter app2.anotherEmbeddedAdapter installed in 0.518 seconds.
```

## Example

A unique identifier for a resource adapter is necessary to identify configured instances of connection factories, administered objects, and activation specifications as being associated with an installed resource adapter. For stand-alone resource adapters, the module name is used as the identifier. For resource adapters embedded in applications, the combination of the application name plus the module name (delimited by the period character) are used as the identifier.

- To specify properties for a stand-alone resource adapter using a `properties.MyAdapter` subelement that includes the resource adapter identifier, `MyAdapter`:  
`<resourceAdapter location="C:/adapters/MyAdapter.rar">`  
`<properties.MyAdapter logFile="${server.output.dir}/logs/myAdapter.log"/>`  
`</resourceAdapter>`
- To associate a connection factory with a stand-alone resource adapter using a `properties.MyAdapter` subelement that includes the resource adapter identifier, `MyAdapter`:  
`<resourceAdapter location="C:/adapters/MyAdapter.rar"/>`  
`<connectionFactory jndiName="eis/cf">`  
`<properties.MyAdapter serverName="localhost" portNumber="1234"/>`  
`</connectionFactory>`
- To associate a connection factory with a resource adapter `MyEmbeddedAdapter`, which is enabled in the `app1` application, using a `properties.app1.MyEmbeddedAdapter` subelement:

```

<application location="C:/applications/app1.ear"/>
<connectionFactory jndiName="eis/cf">
  <properties.appl.MyEmbeddedAdapter serverName="localhost" portNumber="1234"/>
</connectionFactory>

```

- In some cases, the module name is not sufficiently unique to serve as the identifier. This might happen, for example, if you install two different versions of the same resource adapter. Alternately, the module name might be unique, but undesirable for use in configuration because it is lengthy or contains non-alphanumeric characters. You can override the resource adapter identifier by specifying the id attribute.

The following example demonstrates how to override the identifier for stand-alone resource adapters:

```

<resourceAdapter id="MyAdapterV1" location="C:/adapters/version-1.0/MyAdapter.rar"/>
<resourceAdapter id="MyAdapterV2" location="C:/adapters/version-2.0/MyAdapter.rar"/>
<connectionFactory jndiName="eis/cf1">
  <properties.MyAdapterV1 serverName="localhost" portNumber="1234"/>
</connectionFactory>
<connectionFactory jndiName="eis/cf2">
  <properties.MyAdapterV2 serverName="localhost" portNumber="1234"/>
</connectionFactory>

```

- The following example demonstrates how to override the identifier for a resource adapter that is embedded in an application. The example changes the identifier to MyEmbeddedRA:

```

<application location="C:/applications/app1.ear">
  <resourceAdapter id="MyEmbeddedAdapter" alias="MyEmbeddedRA"/>
</application>
<connectionFactory jndiName="eis/cf">
  <properties.appl.MyEmbeddedRA serverName="localhost" portNumber="1234"/>
</connectionFactory>

```

- To compute the module name for embedded resource adapters, the <module-name> entry in the resource adapter deployment descriptor (ra.xml) takes precedence as the module name. For example, given the following definition in ra.xml:

```

<connector ...>
  <module-name>MyRARModule</module-name>
</connector>

```

the module name would be set to "MyRARModule".

If the module name is absent from the connector deployment descriptor, the short form of the URI referring to the resource adapter module in the application deployment descriptor (application.xml) is used. For example, given the following module definition in application.xml:

```

<module>
  <connector>connectors/MyRARModule.rar</connector>
</module>

```

the module name would be computed as "MyRARModule".

If multiple resource adapters are embedded in an application and define the same <module-name> value, the first one listed in application.xml uses that module name. The module names of the other connectors with that same conflicting name are calculated from the full form of the URI with all / (forward slash) characters converted to a period (.). For example, if two connectors were embedded in an application both containing the following definition in ra.xml:

```

<connector ...>
  <module-name>MyRARModule</module-name>
</connector>

```

and the following definitions in application.xml:

```

<module>
  <connector>subfolder1/connector1.rar</connector>
</module>
<module>
  <connector>subfolder2/connector2.rar</connector>
</module>

```

The module name for the first connector would be "MyRARModule" and the module name for the second would be "subfolder2.connector2.rar"



You can configure connection factories that comply with Java EE Connector Architecture (JCA) specification.

### About this task

You can configure one or more connection factory instances for connection factory types that are provided by an installed resource adapter.

**Note:** To configure JCA support for the Liberty profile, you must edit the `server.xml` file using either the Source view of the Server configuration editor of the WebSphere® Application Server Developer Tools for Eclipse, or some other text editor. This topic assumes that a resource adapter with a unique identifier of `MyAdapter` has already been configured in the server, see the documentation on configuring resource adapters for further details. An end-to-end example of configuring a basic scenario is provided in the following steps.

**Note:** Editing the properties sub-elements of the server configuration for connection factories, administrative objects, activation specifications, and resource adapters in the Design view of WebSphere® Development Tools (WDT) is not supported.

### Procedure

1. Update the `server.xml` file to add the `jca-1.6` feature under the `featureManager` tag.

```
<featureManager>
  <feature>jca-1.6</feature>
  <feature>jndi-1.0</feature> <!-- Add the jndi feature to enable look up of connection factories and administered objects -->
  ...
</featureManager>
```

2. Install a resource adapter. For example, update the `server.xml` file as follows:

```
<resourceAdapter location="C:/adapters/MyAdapter.rar"/>
```

3. Configure one or more connection factory instances. When you configure the connection factory instances, you must supply a `properties` subelement, even if you do not want to override any configuration properties, in order to associate the `connectionFactory` element with a connection factory interface that is provided by a particular resource adapter. In the following example, the `MyAdapter` resource adapter provides only one type of connection factory:

```
<connectionFactory jndiName="eis/cf1">
  <properties.MyAdapter portNumber="1234" someVendorProperty="100"/>
</connectionFactory>
```

```
<connectionFactory jndiName="eis/cf2" containerAuthDataRef="auth2">
  <connectionManager maxPoolSize="20" connectionTimeout="0"/>
  <properties.MyAdapter portNumber="1234" someVendorProperty="200"/>
</connectionFactory>
<authData id="auth2" user="user2" password="{xor}Lz4sLCgwLTtt"/>
```

4. (Optional) If required, identify the available connection factory property subelement names.
  - If a resource adapter provides exactly one connection factory interface, excluding any JMS connection factories, the subelement is: `properties.<rar_identifier>`
  - If the interface name is unique without the package name, the subelement name is: `properties.<rar_identifier>.<InterfaceName>`
  - If the implementation name is unique without the package name, the subelement name is: `properties.<rar_identifier>.<ImplementationName>`
  - In other cases, the subelement name is: `properties.<rar_identifier>.<fully.qualified.InterfaceName>`

## Example

Use the following example to learn how to configure resource adapters with two connection factories with unique interface class names.

In the following snippet from a ra.xml file, the MyAdapter resource adapter provides two connection factories with unique interface class names:

```
<connection-definition>
  <config-property>
    <config-property-name>ServerName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
  </config-property>
  <connectionfactory-interface>javax.resource.cci.ConnectionFactory</connectionfactory-interface>
  <connectionfactory-impl-class>com.vendor.adapter.ConnectionFactoryImpl</connectionfactory-impl-class>
</connection-definition>
<connection-definition>
  <config-property>
    <config-property-name>ServerName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
  </config-property>
  <connectionfactory-interface>javax.sql.DataSource</connectionfactory-interface>
  <connectionfactory-impl-class>com.vendor.adapter.DataSourceImpl</connectionfactory-impl-class>
</connection-definition>
```

The following is an example of a server configuration for this scenario:

```
<connectionFactory jndiName="eis/cf">
  <properties.MyAdapter.ConnectionFactory serverName="localhost"/>
</connectionFactory>

<connectionFactory jndiName="jdbc/ds">
  <properties.MyAdapter.DataSource serverName="localhost"/>
</connectionFactory>
```

Use the following example to learn how to configure resource adapters with two connection factories with unique implementation class names.

In the following snippet from a ra.xml file, the MyAdapter resource adapter provides two connection factories with unique implementation class names:

```
<connection-definition>
  <config-property>
    <config-property-name>ServerName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
  </config-property>
  <connectionfactory-interface>javax.resource.cci.ConnectionFactory</connectionfactory-interface>
  <connectionfactory-impl-class>com.vendor.adapter.ConnectionFactoryImpl</connectionfactory-impl-class>
</connection-definition>
<connection-definition>
  <config-property>
    <config-property-name>ServerName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
  </config-property>
  <connectionfactory-interface>com.vendor.adapter.ConnectionFactory</connectionfactory-interface>
  <connectionfactory-impl-class>com.vendor.adapter.MyConnectionFactoryImpl</connectionfactory-impl-class>
</connection-definition>
```

The following is an example of a server configuration for this scenario:

```
<connectionFactory jndiName="eis/cf1">
  <properties.MyAdapter.ConnectionFactoryImpl serverName="localhost"/>
</connectionFactory>
```

```
<connectionFactory jndiName="eis/cf2">
  <properties.MyAdapter.MyConnectionFactoryImpl serverName="localhost"/>
</connectionFactory>
```

Use the following example to learn how to configure resource adapters with two connection factories where neither the simple interface nor implementation class names are unique.

In the following snippet from a ra.xml file, the MyAdapter resource adapter provides two connection factories where neither the simple interface nor the implementation class names are unique:

```
<connection-definition>
  <config-property>
    <config-property-name>ServerName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
  </config-property>
  <connectionfactory-interface>javax.resource.cci.ConnectionFactory</connectionfactory-interface>
  <connectionfactory-impl-class>com.vendor.adapter.ConnectionFactoryImpl</connectionfactory-impl-class>
</connection-defintion>

<connection-definition>
  <config-property>
    <config-property-name>HostName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
  </config-property>
  <connectionfactory-interface>com.vendor.adapter.custom.ConnectionFactory</connectionfactory-interface>
  <connectionfactory-impl-class>com.vendor.adapter.custom.ConnectionFactoryImpl</connectionfactory-impl-class>
</connection-defintion>
```

The following is an example of a server configuration for this scenario:

```
<connectionFactory jndiName="eis/cci-cf">
  <properties.MyAdapter.javax.resource.cci.ConnectionFactory serverName="localhost"/>
</connectionFactory>

<connectionFactory jndiName="eis/custom-cf">
  <properties.MyAdapter.com.vendor.adapter.custom.ConnectionFactory hostName="localhost"/>
</connectionFactory>
```

It is possible to override the suffixes of configuration element names. See the information about customizing JCA configuration elements to learn how to override the suffixes of configuration element names.

## Configuring JCA administered objects: 8.5.5.2

You can configure administered objects that comply with the Java EE Connector Architecture (JCA) specification.

### About this task

You can configure one or more instances of administered objects that are provided by an installed resource adapter.

**Note:** To configure JCA support for Liberty, you must edit the server.xml file using either the Source view of the Server configuration editor of the WebSphere® Application Server Developer Tools for Eclipse, or some other text editor. This topic assumes that a resource adapter with a unique identifier of MyAdapter has already been configured in the server, see the documentation on configuring resource adapters for further details. An end-to-end example of configuring a basic scenario is provided in the following steps.

**Note:** Editing the properties sub-elements of the server configuration for connection factories, administrative objects, activation specifications, and resource adapters in the Design view of WebSphere® Development Tools (WDT) is not supported.

### Procedure

1. Update the server.xml file to add the jca-1.6 feature under the featureManager tag.

```
<featureManager>
  <feature>jca-1.6</feature>
  <feature>jndi-1.0</feature>  <!-- Add the jndi feature to enable look up of connection factories and administered ob
  ...
</featureManager>
```

2. Install a resource adapter. For example, update the server.xml file as follows:

```
<resourceAdapter location="C:/adapters/MyAdapter.rar"/>
```

3. Configure one or more administered object instances. When you configure administered object instances, you must supply a properties subelement, even if you do not want to override any configuration properties, to associate the adminObject element with an administered object type that is provided by a particular resource adapter. In the following example, the MyAdapter resource adapter provides only one type of administered object:

```
<adminObject jndiName="eis/interactionSpec">
  <properties.MyAdapter functionName="find" executionTimeout="5000"/>
</adminObject>
```

4. (Optional) If required, identify the available administered object property subelement names.

- If a resource adapter provides exactly one administered object interface excluding any JMS destinations, queues and topics, the subelement name is: properties.<rar\_identifier>
- If the interface name is unique without the package name, the subelement name is: properties.<rar\_identifier>.<InterfaceName>
- If the implementation name is unique without the package name, the subelement name is: properties.<rar\_identifier>.<ImplementationName>
- If the combination of interface name and implementation name are unique without the package name, the subelement name is: properties.<rar\_identifier>.<InterfaceName>-<ImplementationName>
- In other cases, the subelement name is: properties.<rar\_identifier>.<fully.qualified.InterfaceName>-<fully.qualified.ImplementationName>

### Example

Use the following example to learn how to configure resource adapters with two administered objects with unique interface class names.

In the following snippet from a ra.xml file, the MyAdapter resource adapter provides two administered objects with unique interface class names:

```
<adminobject>
<adminobject-interface>javax.resource.cci.ConnectionSpec</adminobject-interface>
<adminobject-class>com.vendor.adapter.ConnectionSpecImpl</adminobject-class>
<config-property>
  <config-property-name>isolationLevel</config-property-name>
  <config-property-type>java.lang.Integer</config-property-type>
</config-property>
...
</adminobject>
```

```
<adminobject>
<adminobject-interface>javax.resource.cci.InteractionSpec</adminobject-interface>
<adminobject-class>com.vendor.adapter.InteractionSpecImpl</adminobject-class>
<config-property>
```

```

    <config-property-name>FunctionName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
</config-property>
...
</adminobject>

```

The following is an example of a server configuration for this scenario:

```

<adminObject jndiName="eis/connectionSpec">
  <properties.MyAdapter.ConnectionSpec isolationLevel="4"/>
</adminObject>

<adminObject jndiName="eis/interactionSpec">
  <properties.MyAdapter.InteractionSpec functionName="find"/>
</adminObject>

```

Use the following example to learn how to configure resource adapters with two administered objects with unique implementation class names.

In the following snippet from a ra.xml file, the MyAdapter resource adapter provides two administered objects with unique implementation class names:

```

<adminobject>
<adminobject-interface>javax.resource.cci.InteractionSpec</adminobject-interface>
<adminobject-class>com.vendor.adapter.FinderInteractionSpec</adminobject-class>
<config-property>
  <config-property-name>ResultSetType</config-property-name>
  <config-property-type>java.lang.Integer</config-property-type>
</config-property>
...
</adminobject>

<adminobject>
<adminobject-interface>javax.resource.cci.InteractionSpec</adminobject-interface>
<adminobject-class>com.vendor.adapter.UpdaterInteractionSpec</adminobject-class>
<config-property>
  <config-property-name>ExecutionTimeout</config-property-name>
  <config-property-type>java.lang.Long</config-property-type>
</config-property>
...
</adminobject>

```

The following is an example of a server configuration for this scenario:

```

<adminObject jndiName="eis/finder">
  <properties.MyAdapter.FinderInteractionSpec resultSetType="1003"/>
</adminObject>

<adminObject jndiName="eis/updater">
  <properties.MyAdapter.UpdaterInteractionSpec executionTimeout="3000"/>
</adminObject>

```

Use the following example to learn how to configure resource adapters with two administered objects where neither the simple interface nor implementation class names are unique.

In the following snippet from a ra.xml file, the MyAdapter resource adapter provides two administered objects where neither the simple interface nor the implementation class names are unique:

```

<adminobject>
<adminobject-interface>javax.resource.cci.InteractionSpec</adminobject-interface>
<adminobject-class>com.vendor.adapter.finder.InteractionSpecImpl</adminobject-class>
<config-property>
  <config-property-name>ResultSetType</config-property-name>
  <config-property-type>java.lang.Integer</config-property-type>
</config-property>
...

```

```

</adminobject>

<adminobject>
<adminobject-interface>javax.resource.cci.InteractionSpec</adminobject-interface>
<adminobject-class>com.vendor.adapter.updater.InteractionSpecImpl</adminobject-class>
<config-property>
  <config-property-name>ExecutionTimeout</config-property-name>
  <config-property-type>java.lang.Long</config-property-type>
</config-property>
...
</adminobject>

```

The following is an example of a server configuration for this scenario:

```

<adminObject jndiName="eis/finder">
  <properties.MyAdapter.javax.resource.cci.InteractionSpec-com.vendor.adapter.finder.InteractionSpecImpl resultSetType="1" />
</adminObject>

<adminObject jndiName="eis/updater">
  <properties.MyAdapter.javax.resource.cci.InteractionSpec-com.vendor.adapter.updater.InteractionSpecImpl executionTimeout="1" />
</adminObject>

```

It is possible to override the suffixes of configuration element names. See the information about customizing JCA configuration elements to learn how to override the suffixes of configuration element names.

### Configuring JCA activation specifications: 8.5.5.2

You can configure activation specifications that comply with the Java EE Connector Architecture (JCA) specification.

#### About this task

You can configure one or more instances of activation specifications that are provided by an installed resource adapter.

**Note:** To configure JCA support for Liberty, you must edit the `server.xml` file using either the Source view of the Server configuration editor of the WebSphere® Application Server Developer Tools for Eclipse, or some other text editor. This topic assumes that a resource adapter with a unique identifier of `MyAdapter` has already been configured in the server, see the documentation on configuring resource adapters for further details. An end-to-end example of configuring a basic scenario is provided in the following steps.

**Note:** Editing the properties sub-elements of the server configuration for connection factories, administrative objects, activation specifications, and resource adapters in the Design view of WebSphere® Development Tools (WDT) is not supported.

#### Procedure

1. Update the `server.xml` file to add the `jca-1.6` feature under the `featureManager` tag.

```

<featureManager>
  <feature>jca-1.6</feature>
  <feature>jndi-1.0</feature> <!-- Add the jndi feature to enable look up of connection factories and administered ob
  ...
</featureManager>

```

2. Install a resource adapter. For example, update the `server.xml` file as follows:

```

<resourceAdapter location="C:/adapters/MyAdapter.rar"/>

```

3. Configure one or more activation specifications. When you configure activation specifications, you must supply a `properties` subelement, even if you do not want to override any configuration

properties, to associate the activationSpec element with a message listener type that is provided by a particular resource adapter. In the following example, the MyAdapter resource adapter provides only one type of message listener:

```
<activationSpec id="app1/module1/MyMessageDrivenBean">
  <properties.MyAdapter messageFilter="ALL"/>
</activationSpec>
```

4. If required, identify the available activation specification property subelement names.
  - If a resource adapter provides exactly one message listener interface, excluding any JMS connection factories, the subelement name is: `properties.<rar_identifier>`
  - If the message listener interface name is unique without the package name, the subelement name is: `properties.<rar_identifier>.<MessageListenerInterfaceName>`
  - If the activation specification implementation name is unique without the package name, the subelement name is: `properties.<rar_identifier>.<ActivationSpecificationImplementationName>`
  - If the activation specification implementation name is unique without the package name, the subelement name is: `properties.<rar_identifier>.<ActivationSpecificationImplementationName>`
  - In other cases, the subelement name is: `properties.<rar_identifier>.<fully.qualified.MessageListenerInterfaceName>`
5. See the documentation on deploying message-driven beans for information about how to associate the activation specification with a message-driven bean.

### Example

Use the following example to learn how to configure resource adapters with two message listener types with unique interface class names.

In the following snippet from a `ra.xml` file, the MyAdapter resource adapter provides two message listener types with unique interface class names:

```
<messageListener>
<messageListener-type>javax.resource.cci.MessageListener</messageListener-type>
<activationSpec>
  <activationSpec-class>com.vendor.adapter.CCIActivationSpec</activationSpec-class>
  <config-property>
    <config-property-name>maxSize</config-property-name>
    <config-property-type>java.lang.Long</config-property-type>
  </config-property>
  ...
</activationSpec>
...
</messageListener>

<messageListener>
<messageListener-type>com.vendor.adapter.MyMessageListener</messageListener-type>
<activationSpec>
  <activationSpec-class>com.vendor.adapter.MyActivationSpec</activationSpec-class>
  <config-property>
    <config-property-name>messageFilter</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
  </config-property>
  ...
</activationSpec>
...
</messageListener>
```

The following is an example of a server configuration for this scenario:

```
<activationSpec id="app1/module1/CCIMessageDrivenBean">
  <properties.MyAdapter.MessageListener maxSize="1024"/>
</activationSpec>
```

```
<activationSpec id="app1/module1/MyMessageDrivenBean">
  <properties.MyAdapter.MyMessageListener messageFilter="ALL"/>
</activationSpec>
```

Use the following example to learn how to configure resource adapters with two message listener types with unique implementation class names

In the following snippet from a ra.xml file, the MyAdapter resource adapter provides two message listener types with unique implementation class names:

```
<messageListener>
<messageListener-type>javax.resource.cci.MessageListener</messageListener-type>
<activationSpec>
  <activationSpec-class>com.vendor.adapter.CCIActivationSpec</activationSpec-class>
  <config-property>
    <config-property-name>maxSize</config-property-name>
    <config-property-type>java.lang.Long</config-property-type>
  </config-property>
  ...
</activationSpec>
...
</messageListener>

<messageListener>
<messageListener-type>com.vendor.adapter.MessageListener</messageListener-type>
<activationSpec>
  <activationSpec-class>com.vendor.adapter.MyActivationSpec</activationSpec-class>
  <config-property>
    <config-property-name>messageFilter</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
  </config-property>
  ...
</activationSpec>
...
</messageListener>
```

The following is an example of a server configuration for this scenario:

```
<activationSpec id="app1/module1/CCIMessageDrivenBean">
  <properties.MyAdapter.CCIActivationSpec maxSize="1024"/>
</activationSpec>

<activationSpec id="app1/module1/MyMessageDrivenBean">
  <properties.MyAdapter.MyActivationSpec messageFilter="ALL"/>
</activationSpec>
```

Use the following example to learn how to configure resource adapters with two message listener types where neither the simple interface nor implementation class names are unique.

In the following snippet from a ra.xml file, the MyAdapter resource adapter provides two message listener types where neither the simple interface nor the implementation class names are unique:

```
<messageListener>
<messageListener-type>javax.resource.cci.MessageListener</messageListener-type>
<activationSpec>
  <activationSpec-class>com.vendor.adapter.cci.ActivationSpec</activationSpec-class>
  <config-property>
    <config-property-name>maxSize</config-property-name>
    <config-property-type>java.lang.Long</config-property-type>
  </config-property>
  ...
</activationSpec>
...
</messageListener>
```

```

<messageListener>
<messageListener-type>com.vendor.adapter.MessageListener</messageListener-type>
<activationSpec>
  <activationSpec-class>com.vendor.adapter.ActivationSpec</activationSpec-class>
  <config-property>
    <config-property-name>messageFilter</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
  </config-property>
  ...
</activationSpec>
  ...
</messageListener>

```

The following is an example of a server configuration for this scenario:

```

<activationSpec id="app1/module1/CCIMessageDrivenBean">
  <properties.MyAdapter.javax.resource.cci.MessageListener maxSize="1024"/>
</activationSpec>

<activationSpec id="app1/module1/MyMessageDrivenBean">
  <properties.MyAdapter.com.vendor.adapter.MessageListener messageFilter="ALL"/>
</activationSpec>

```

It is possible to override the suffixes of configuration element names. See the information about customizing JCA configuration elements to learn how to override the suffixes of configuration element names.

## Configuring JMS connection factories: 8.5.5.2

You can configure JMS connection factories that are provided by resource adapters that comply with the Java EE Connector Architecture (JCA) specification.

### About this task

You can configure one or more JMS connection factory instances for JMS connection factory types that are provided by an installed resource adapter.

Configuration elements are provided for the following types of JMS connection factories:

- javax.jms.ConnectionFactory: jmsConnectionFactory
- javax.jms.QueueConnectionFactory: jmsQueueConnectionFactory
- javax.jms.TopicConnectionFactory: jmsTopicConnectionFactory

### Note:

To add JCA support for Liberty, you must edit the `server.xml` file using either the Source view of the Server configuration editor of the WebSphere® Application Server Developer Tools for Eclipse, or some other text editor. Editing portions of the configuration for connection factories, administrative objects, activation specifications, and resource adapters in the Design view is not supported in the Beta.

### Procedure

Configure one or more JMS connection factory instances. When you configure the connection factory instances, you must supply a `properties` subelement, even if you do not want to override any configuration properties, to associate the `jmsConnectionFactory`, `jmsQueueConnectionFactory`, or `jmsTopicConnectionFactory` element with a connection factory interface that is provided by a particular resource adapter. The `properties` subelement always follows the pattern `properties.<rar_identifier>` for JMS connection factories. In the following example, the `MyAdapter` resource adapter provides only one type of connection factory:

```

<jmsConnectionFactory jndiName="jms/cf" containerAuthDataRef="auth1">
  <properties.MyAdapter serverName="localhost" anotherProperty="40"/>
</jmsConnectionFactory>
<authData id="auth1" user="user1" password="{xor}Lz4sLCgwLTtu"/>

<jmsQueueConnectionFactory jndiName="jms/qcf">
  <connectionManager maxPoolSize="20" connectionTimeout="0"/>
  <properties.MyAdapter serverName="localhost" vendorProp1="1"/>
</jmsQueueConnectionFactory>

<jmsTopicConnectionFactory jndiName="jms/tcf">
  <properties.MyAdapter serverName="localhost" prop1="A" prop2="B"/>
</jmsTopicConnectionFactory>

```

**Note:** This topic assumes that a resource adapter with a unique identifier of MyAdapter has already been configured in the server and that the `jms-1.1` feature has been enabled. See topic “Configuring resource adapters” on page 1615 for further details.

Limitation: Editing the properties of the resource adapter configuration for connection factories, administrative objects, activation specifications, and resource adapters in the Design view of WebSphere Development Tools (WDT) is not supported.

## Configuring JMS destinations: 8.5.5.2

You can configure JMS destinations that are provided by resource adapters that comply with the Java EE Connector Architecture (JCA) specification.

### About this task

You can configure one or more instances of JMS destination, queue, or topic types that are provided by an installed resource adapter.

Configuration elements are provided for the following types of JMS destinations:

- `javax.jms.Destination`: `jmsDestination`
- `javax.jms.Queue`: `jmsQueue`
- `javax.jms.Topic`: `jmsTopic`

### Note:

To add JCA support for Liberty, you must edit the `server.xml` file using either the Source view of the Server configuration editor of the WebSphere® Application Server Developer Tools for Eclipse, or some other text editor. Editing portions of the configuration for connection factories, administrative objects, activation specifications, and resource adapters in the Design view is not supported in the Beta.

### Procedure

1. Configure one or more JMS destination, queue, or topic instances. When you configure the destination instances, you must supply a `properties` subelement, even if you do not want to override any configuration properties, to associate the `jmsDestination`, `jmsQueue`, or `jmsTopic` element with a JMS destination interface that is provided by a particular resource adapter. In the following example, the MyAdapter resource adapter provides only one type of JMS destination, one type of JMS queue, and one type of JMS topic:

```

<jmsDestination jndiName="jms/destination1">
  <properties.MyAdapter name="DEST1"/>
</jmsDestination>

<jmsQueue jndiName="jms/queue1">
  <properties.MyAdapter queueName="QUEUE1"/>

```

```

</jmsQueue>

<jmsTopic id="topic1" jndiName="jms/topic1">
  <properties.MyAdapter topicName="TOPIC1"/>
</jmsTopic>

```

- (Optional) If required, identify the available destination, queue, and topic property subelement names.

**Note:** This topic assumes that a resource adapter with a unique identifier of MyAdapter has already been configured in the server. See topic “Configuring resource adapters” on page 1615 for further details.

Limitation: Editing the properties of the resource adapter configuration for connection factories, administrative objects, activation specifications, and resource adapters in the Design view of WebSphere Development Tools (WDT) is not supported.

- If a resource adapter provides exactly one type of administered object with the `javax.jms.Destination` interface, the subelement name is: `properties.<rar_identifier>`
- If the implementation name is unique without the package name the subelement name is: `properties.<rar_identifier>.<ImplementationName>`
- In other cases, the subelement name is: `properties.<rar_identifier>.<fully.qualified.InterfaceName>`
- If a resource adapter provides exactly one type of administered object with the `javax.jms.Queue` interface, the subelement name is: `properties.<rar_identifier>`
- If the implementation name is unique without the package name, the subelement name is: `properties.<rar_identifier>.<ImplementationName>`
- In other cases, the subelement name is: `properties.<rar_identifier>.<fully.qualified.InterfaceName>`
- If a resource adapter provides exactly one type of administered object with the `javax.jms.Topic` interface, the subelement name is: `properties.<rar_identifier>`
- If the implementation name is unique without the package name, the subelement name is: `properties.<rar_identifier>.<ImplementationName>`
- In other cases, the subelement name is: `properties.<rar_identifier>.<fully.qualified.InterfaceName>`

## Example

Use the following example to learn how to configure resource adapters with two JMS destinations with unique implementation class names

In the following snippet from a `ra.xml` file the MyAdapter resource adapter provides two JMS destinations with unique implementation class names:

```

<adminobject>
<adminobject-interface>javax.jms.Destination</adminobject-interface>
<adminobject-class>com.vendor.adapter.QueueImpl</adminobject-class>
<config-property>
  <config-property-name>queueName</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
</config-property>
  ...
</adminobject>

<adminobject>
<adminobject-interface>javax.jms.Destination</adminobject-interface>
<adminobject-class>com.vendor.adapter.TopicImpl</adminobject-class>
<config-property>
  <config-property-name>topicName</config-property-name>

```

```

    <config-property-type>java.lang.String</config-property-type>
  </config-property>
  ...
</adminobject>

```

The following is an example of a server configuration for this scenario:

```

<jmsDestination jndiName="jms/destination1">
  <properties.MyAdapter.QueueImpl queueName="D1"/>
</adminObject>

<jmsDestination jndiName="jms/destination2">
  <properties.MyAdapter.TopicImpl topicName="D2"/>
</jmsDestination>

```

Use the following example to learn how to configure resource adapters with two administered objects without implementation class names that are unique.

In the following snippet from a ra.xml file the MyAdapter resource adapter provides two administered objects with non-unique implementation class names:

```

<adminobject>
<adminobject-interface>javax.jms.Queue</adminobject-interface>
<adminobject-class>com.vendor.adapter.QueueImpl</adminobject-class>
<config-property>
  <config-property-name>queueName</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
</config-property>
...
</adminobject>

<adminobject>
<adminobject-interface>javax.jms.Queue</adminobject-interface>
<adminobject-class>com.vendor.adapter.advanced.QueueImpl</adminobject-class>
<config-property>
  <config-property-name>name</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
</config-property>
...
</adminobject>

```

The following is an example of a server configuration for this scenario:

```

<jmsQueue jndiName="jms/myQueue">
  <properties.MyAdapter.com.vendor.adapter.QueueImpl queueName="Q1"/>
</jmsQueue>

<jmsQueue jndiName="jms/myAdvancedQueue">
  <properties.MyAdapter.com.vendor.adapter.advanced.QueueImpl name="Q1"/>
</jmsQueue>

```

In some scenarios, lengthy configuration element names might be undesirable. See the information about customizing JCA configuration elements to learn how to override the suffixes of configuration element names.

### Configuring JMS activation specifications: 8.5.5.2

You can configure JMS activation specifications that are provided by resource adapters that comply with the Java EE Connector Architecture (JCA) specification.

#### About this task

You can configure one or more JMS activation specification instances for JMS message listeners that are provided by an installed resource adapter.

**Note:**

To add JCA support for Liberty, you must edit the `server.xml` file using either the Source view of the Server configuration editor of the WebSphere® Application Server Developer Tools for Eclipse, or some other text editor. Editing portions of the configuration for connection factories, administrative objects, activation specifications, and resource adapters in the Design view is not supported in the Beta.

**Procedure**

Configure one or more JMS activation specification instances. When you configure the activation specification instances, you must supply a `properties` subelement, even if you do not want to override any configuration properties, to associate the `jmsActivationSpec` element with a JMS message listener that is provided by a particular resource adapter. The `properties` subelement always follows the pattern `properties`, `<rar_identifier>` for JMS activation specifications. The following example configures two instances of JMS activation specifications:

```
<jmsActivationSpec id="app1/module1/MyJMSMessageDrivenBean">
  <properties.MyAdapter destinationRef="topic1"/>
</jmsActivationSpec>

<jmsActivationSpec id="app1/module1/AnotherJMSMessageDrivenBean">
  <containerAuthData user="user1" password="{xor}Lz4sLCgwLTtu"/>
  <properties.MyAdapter destinationRef="queue1"/>
</jmsActivationSpec>
```

**Note:** This topic assumes that a resource adapter with a unique identifier of `MyAdapter` has already been configured in the server and that the `jms-1.1` and `mdb-3.1` features have been enabled. See topic “Configuring resource adapters” on page 1615 for further details.

Limitation: Editing the properties of the resource adapter configuration for connection factories, administrative objects, activation specifications, and resource adapters in the Design view of WebSphere Development Tools (WDT) is not supported.

**Customizing JCA configuration elements:** 8.5.5.2 

You can customize how JCA properties subelements are generated when installing a resource adapter.

**About this task**

When you install a stand-alone resource adapter or a resource adapter that is embedded in an application, you can add one or more `<customize>` subelements under the `<resourceAdapter>` element to choose the suffix that is used for the `properties` subelement for the specified interface or implementation class. Customizing subelement enables you to avoid lengthy `properties` subelement names that might otherwise be required for the configuration elements to have unique names.

**Note:**

To add JCA support for Liberty, you must edit the `server.xml` file using either the Source view of the Server configuration editor of the WebSphere® Application Server Developer Tools for Eclipse, or some other text editor. Editing portions of the configuration for connection factories, administrative objects, activation specifications, and resource adapters in the Design view is not supported in the Beta.

**Procedure**

1. For a stand-alone resource adapter, start with the existing configuration that you want to customize. For example, if a resource adapter `MyAdapter` provides two connection factories, where neither the simple interface nor implementation class names are unique:

```

<featureManager>
  <feature>jca-1.6</feature>
  <feature>jndi-1.0</feature> <!-- Add the jndi feature to enable look up of connection factories and administered ob
  ...
</featureManager>
<resourceAdapter location="C:/adapters/MyAdapter.rar"/>

<connectionFactory jndiName="eis/cci-cf">
  <properties.MyAdapter.javax.resource.cci.ConnectionFactory serverName="localhost"/>
</connectionFactory>

<connectionFactory jndiName="eis/custom-cf">
  <properties.MyAdapter.com.vendor.adapter.custom.ConnectionFactory hostName="localhost"/>
</connectionFactory>

```

2. Add customize subelements to the resourceAdapter to choose the suffixes for both of the connection factory interfaces.

```

<featureManager>
  <feature>jca-1.6</feature>
  <feature>jndi-1.0</feature> <!-- Add the jndi feature to enable look up of connection factories and administered ob
  ...
</featureManager>

<resourceAdapter location="C:/adapters/MyAdapter.rar">
  <customize interface="javax.resource.cci.ConnectionFactory" suffix="cci"/>
  <customize interface="com.vendor.adapter.custom.ConnectionFactory" suffix="custom"/>
</resourceAdapter>

<connectionFactory jndiName="eis/cci-cf">
  <properties.MyAdapter.cci serverName="localhost"/>
</connectionFactory>

<connectionFactory jndiName="eis/custom-cf">
  <properties.MyAdapter.custom hostName="localhost"/>
</connectionFactory>

```

3. For a resource adapter that is embedded in an application, start with the existing configuration that you want to customize. For example, assume that you have an application app1 with an embedded resource adapter named MyAdapter as follows:

```

<featureManager>
  <feature>jca-1.6</feature>
  <feature>jndi-1.0</feature> <!-- Add the jndi feature to enable look up of connection factories and administered ob
  ...
</featureManager>

<application name="app1" type="ear" location="C:/applications/app1.ear"/>

<adminObject jndiName="eis/interactionSpec-find">
  <properties.app1.MyAdapter.javax.resource.cci.InteractionSpec-com.vendor.adapter.finder.InteractionSpecImpl resultSe
</adminObject>

<adminObject jndiName="eis/interactionSpec-update">
  <properties.app1.MyAdapter.com.vendor.adapter.InteractionSpec-com.vendor.adapter.updater.InteractionSpecImpl executi
</adminObject>

```

4. Specify a resourceAdapter element for the Resource Adapter Archive (RAR) module in the application. Specify the id attribute to be the module name of the RAR module. Add customize subelements to choose the suffixes for both of the administered objects that are based on the interface or implementation class. In this example, only the implementation class is specified, which is sufficient to identify the administered objects:

```

<featureManager>
  <feature>jca-1.6</feature>
  <feature>jndi-1.0</feature> <!-- Add the jndi feature to enable look up of connection factories and administered ob
  ...
</featureManager>

```

```

<application name="app1" type="ear" location="C:/applications/app1.ear">
  <resourceAdapter id="MyAdapter">
    <customize implementation="com.vendor.adapter.finder.InteractionSpecImpl" suffix="finder"/>
    <customize implementation="com.vendor.adapter.updater.InteractionSpecImpl" suffix="updater"/>
  </resourceAdapter>
</application>

<adminObject jndiName="eis/interactionSpec-find">
  <properties.app1.MyAdapter.finder resultSetType="1003"/>
</adminObject>

<adminObject jndiName="eis/interactionSpec-update">
  <properties.app1.MyAdapter.updater executionTimeout="3000"/>
</adminObject>

```

## Accessing stand-alone resource adapters from Java EE applications:

8.5.5.2



You can access stand-alone resource adapters from Java EE applications.

### About this task

Stand-alone resource adapter classes and resources can be shared across multiple Java EE applications. By default, Java EE applications have access to JCA spec API but do not have access to the vendor classes and resources of stand-alone resource adapters. A prerequisite of enabling this access is that both the resource adapter and the application must be configured in the server configuration.

In the following example, an application called Scholar and an application called Student are running on a server called Academy. Both applications need access to a resource adapter called Socrates16, which is provided in the socrates.rar file that is located in the C:/adapters/version-1.6 directory.

### Procedure

1. Configure the stand-alone resource adapter.

In the server.xml file, configure the stand-alone resource adapter by adding the following code:

```
<resourceAdapter id="Socrates16" location="C:/adapters/version-1.6/socrates.rar" />
```

2. Reference the resource adapter from the applications so that both applications can access the classes and resources that are provided in the resource adapter module.

In the server.xml file, set the classProviderRef attribute to the ID of the resource adapter within the class loading configurations of the applications by adding the following code:

```

<application id="scholar" name="Scholar" type="ear" location="scholar.ear">
  <classloader classProviderRef="Socrates16" />
</application>

```

```

<application id="student" name="Student" type="ear" location="student.ear">
  <classloader classProviderRef="Socrates16" />
</application>

```

3. Optional: Configure the class loading of the stand-alone resource adapter to access third-party APIs. By default, neither resource adapters nor Java applications can access third-party APIs. Whenever the class loading configuration of an application requires access to third-party APIs and the application requires access to a stand-alone resource adapter, configure the class loading of the resource adapter to also access third-party APIs.

In the server.xml file, configure the apiTypeVisibility attribute of the class loading configuration of the resource adapter to access third-party APIs by adding the following code:

```

<resourceAdapter id="Socrates16" location="C:/adapters/version-1.6/socrates.rar">
  <classloader apiTypeVisibility="spec, ibm-api, api, third-party" />
</resourceAdapter/>

```

```
<application id="scholar" name="Scholar" type="ear" location="scholar.ear">
```

```

    <classloader classProviderRef="Socrates16" apiTypeVisibility="spec, ibm-api, api, third-party" />
</application>

<application id="student" name="Student" type="ear" location="student.ear">
  <classloader classProviderRef="Socrates16" apiTypeVisibility="spec, ibm-api, api, third-party" />
</application>

```

## Configuring ManagedExecutorService instances

You can configure `ManagedExecutorService` instances to run asynchronous tasks with the specified thread context. It is a best practice for Java EE applications to avoid directly managing their own threads; therefore, the `ManagedExecutorService` extends the JSE `ExecutorService` to provide a way to launch asynchronous tasks within an application server environment. You might also configure the `ManagedExecutorService` to propagate various thread contexts that are relevant to Java EE applications to the thread of the asynchronous task.

### 8.5.5.0

#### About this task

The `ManagedExecutorService` is available under the `<concurrent-1.0>` feature and enabled in the `server.xml` file as follows:

```

<featureManager>
  <feature>concurrent-1.0</feature>
</featureManager>

```

Propagation of context to the thread of a task that is executed by the `ManagedExecutorService` is managed by the context service. A default instance of the context service (`DefaultContextService`) is created by the server and configured to propagate at least `classloaderContext`, `jeeMetadataContext` and `securityContext`. This default context service instance is used if a `ManagedExecutorService` is created without referring to a specific context service instance or configuring a context service instance directly within. Refer to the [Configuring thread context service instances](#) topic for more information.

A default managed executor instance (`DefaultManagedExecutorService`) is available as `java:comp/DefaultManagedExecutorService` and uses the default context service instance for thread context capture and propagation.

#### Procedure

Example configuration in the `server.xml` file:

- Managed executor service instance that is registered in JNDI with the name `concurrent/execSvc`, and that uses the default context service instance:

```

<managedExecutorService jndiName="concurrent/execSvc"/>

```

- Managed executor service instance with context service configured to propagate `jeeMetadataContext` only:

```

<managedExecutorService jndiName="concurrent/execSvc1">
  <contextService>
    <jeeMetadataContext/>
  </contextService>
</managedExecutorService>

```

- Managed executor service instance with `classloaderContext` and `securityContext`:

```

<managedExecutorService jndiName="concurrent/execSvc2">
  <contextService>
    <classloaderContext/>
    <securityContext/>
  </contextService>
</managedExecutorService>

```

- Thread context service that is shared by multiple managed executor service instances:

```
<contextService id="contextSvc1">
  <jeeMetadataContext/>
</contextService>
```

```
<managedExecutorService jndiName="concurrent/execSvc3" contextServiceRef="contextSvc1"/>
```

```
<managedExecutorService jndiName="concurrent/execSvc4" contextServiceRef="contextSvc1"/>
```

- Thread context service that inherits from the previous example and is used by a managed executor service instance:

```
<contextService id="contextSvc2" baseContextRef="contextSvc1">
  <classloaderContext/>
</contextService>
```

```
<managedExecutorService jndiName="concurrent/execSvc5" contextServiceRef="contextSvc2"/>
```

- Managed executor service instance with `zosWLMContext` plus thread context propagation inherited from the default context service instance:

```
<managedExecutorService jndiName="concurrent/execSvc6">
  <contextService baseContextRef="DefaultContextService">
    <zosWLMContext defaultTransactionClass="TRAN1"/>
  </contextService>
</managedExecutorService>
```

## Example

Managed executor serviced instances can be injected into application components (by using `@Resource`) or looked up with resource environment references (`resource-env-ref`). Regardless of how the instance is obtained, you can use it interchangeably as `javax.enterprise.concurrent.ManagedExecutorService` or its `java.util.concurrent.ExecutorService` superclass.

- Example that looks up the default managed executor:

```
ManagedExecutorService executor =
    (ManagedExecutorService) new InitialContext().lookup(
        "java:comp/DefaultManagedExecutorService");
executor.submit(doSomethingInParallel);
```

- Example that uses `@Resource` to inject as `java.util.concurrent.ExecutorService`:

```
@Resource(lookup="concurrent/execSvc1")
ExecutorService execSvc1;
```

```
...
```

```
// submit task to run
Future<Integer> future1 = execSvc1.submit(new Callable<Integer>() {
    public Integer call() throws Exception {
        // java:comp lookup is possible because <jeeMetadataContext> is configured
        DataSource ds = (DataSource) new InitialContext().lookup("java:comp/env/jdbc/ds1");
        ... make updates to the database
        return updateCount;
    }
});
Future<Integer> future2 = execSvc1.submit(anotherTaskThatUpdatesADatabase);
```

```
numUpdatesCompleted = future1.get() + future2.get();
```

- Example that uses `@Resource` to inject as `javax.enterprise.concurrent.ManagedExecutorService`:

```
@Resource(lookup="concurrent/execSvc1")
ManagedExecutorService execSvc1;
```

```
...
```

```
// submit task to run
Future<Integer> future1 = execSvc1.submit(new Callable<Integer>() {
```

```

public Integer call() throws Exception {
    // java:comp lookup is possible because <jeeMetadataContext> is configured
    DataSource ds = (DataSource) new InitialContext().lookup("java:comp/env/jdbc/ds1");
    ... make updates to the database
    return updateCount;
}
});
Future<Integer> future2 = execSvc1.submit(anotherTaskThatUpdatesADatabase);

```

```
numUpdatesCompleted = future1.get() + future2.get();
```

- Example <resource-env-ref> for java.util.concurrent.ExecutorService in the web.xml file:

```

<resource-env-ref>
  <resource-env-ref-name>concurrent/execSvc2</resource-env-ref-name>
  <resource-env-ref-type>java.util.concurrent.ExecutorService</resource-env-ref-type>
</resource-env-ref>

```

- Example <resource-env-ref> for javax.enterprise.concurrent.ManagedExecutorService in the web.xml file:

```

<resource-env-ref>
  <resource-env-ref-name>concurrent/execSvc2</resource-env-ref-name>
  <resource-env-ref-type>javax.enterprise.concurrent.ManagedExecutorService</resource-env-ref-type>
</resource-env-ref>

```

- Example lookup that uses a resource environment reference:

```

ExecutorService execSvc2 =
    (ExecutorService) new InitialContext().lookup("java:comp/env/concurrent/execSvc2");

futures = execSvc2.invokeAll(Arrays.asList(task1, task2, task3));

```

- Example lookup that uses a resource environment reference and casts to ManagedExecutorService:

```

ManagedExecutorService execSvc2 =
    (ManagedExecutorService) new InitialContext().lookup("java:comp/env/concurrent/execSvc2");

futures = execSvc2.invokeAll(Arrays.asList(task1, task2, task3));

```

## Configuring thread context service instances

8.5.5.4

You can configure ContextService instances to capture a managed thread context and apply it to invocations of specified interface methods on any thread.

### About this task

It is a best practice for Java EE applications to avoid directly managing their own threads; therefore, the ContextService provides a way to establish a previously captured thread context onto unmanaged threads, as well as managed threads, overlaying any thread context that is in place.

A default thread context service instance (DefaultContextService) is created by the server and configured to capture and propagate at least classloaderContext, jeeMetadataContext and securityContext. You can configure thread context propagation to include the following types of thread context:

#### classloaderContext

Makes the thread context classloader of the submitter of the task available to the task.    
8.5.5.4 If the context classloader is serialized, the classloader must be a thread context classloader from the application. Classloader serialization for Web Application Bundles is not currently supported.

#### jeeMetadataContext

Makes the namespace of the application component that submitted the task available to the task.

## securityContext

**8.5.5.4** You must enable the appSecurity-2.0 feature in the server.xml file to use this type of thread context. Makes the caller subject and invocation subject of the submitter of the task available to the task, and this is accomplished by logging in with the submitter's WSPincipal using JAAS login. For details on what information in the submitter's subject is not in the security context, see the concurrent-1.0 feature restrictions.

z/OS

## syncToOSThreadContext

Synchronizes the identity of the runAs Subject for the unit of work with the operating system identity.

z/OS

## zosWLMContext

Used to classify work.

**Important:** Additional thread context providers might be made available by features in stack products. The optional baseContextRef attribute allows a context service instance to inherit from the context configuration of another context service instance.

## Procedure

Enable the thread context service in the server.xml file. The thread context service is available under the <concurrent-1.0> feature.

```
<featureManager>
  <feature>concurrent-1.0</feature>
</featureManager>
```

## Example

Configure thread context service instances in the server.xml file:

- Thread context service that is registered in JNDI with the name, concurrent/threadContextSvc1, that captures and propagates jeeMetadataContext only:

```
<contextService id="threadContextSvc1" jndiName="concurrent/${id}">
  <jeeMetadataContext/>
</contextService>
```

- Thread context service with classloaderContext and securityContext:

```
<contextService jndiName="concurrent/threadContextSvc2">
  <classloaderContext/>
  <securityContext/>
</securityContext/>
```

- Thread context service that inherits jeeMetadataContext from threadContextSvc1 and adds securityContext:

```
<contextService jndiName="concurrent/threadContextSvc3"
baseContextRef="threadContextSvc1">
  <securityContext>
</contextService>
```

Example that looks up the default context service:

```
ContextService threadContextSvc =
  (ContextService) new InitialContext().lookup(
    "java:comp/DefaultContextService");
myContextualAsyncCallback = threadContextSvc.createContextualProxy(
  myAsyncCallback, MyAsyncCallback.class);
doSomethingAsync(arg1, arg2, myContextualAsyncCallback);
```

Examples to inject thread context service instances into application components (by using @Resource) or look up with resource environment references (resource-env-ref).

- Example that uses @Resource:

```
@Resource(lookup="concurrent/threadContextSvc1")
ContextService threadContextSvc1;

...

Callable<Integer> processSalesOrderCompletion = new Callable<Integer>() {
    public Integer call() throws Exception {
        DataSource ds = (DataSource) new InitialContext().lookup("java:comp/env/jdbc/ds1");
        ...update various database tables
        return isSuccessful;
    }
};
// capture thread context of current application component
execProps = Collections.singletonMap(ManagedTask.TRANSACTION,
ManagedTask.USE_TRANSACTION_OF_EXECUTION_THREAD);
processSalesOrderCompletion = (Callable<Boolean>)
    threadContextSvc1.createContextualProxy(processSaleCompletion, execProps,
Callable.class);

//later from a different application component
tran.begin();
...
successful = processSalesOrderCompletion.call();
if (successful)
    tran.commit();
else
    tran.rollback();
```

- Example that specifies resource-env-ref in the web.xml file:

```
<resource-env-ref>
  <resource-env-ref-name>concurrent/threadContextSvc3</resource-env-ref-name>
  <resource-env-ref-type>javax.enterprise.concurrent.ContextService</resource-
env-ref-type>
</resource-env-ref>
```

- Example lookup that uses the resource environment reference:

```
ContextService threadContextSvc3 =
(ContextService) new InitialContext().lookup("java:comp/env/concurrent/threadContextSvc3");
Runnable updateAndGetNextFromDatabase = threadContextSvc3.createContextualProxy
(new Runnable() {
    public void run() {
        DataSource ds = (DataSource) new InitialContext().lookup("java:comp/env/jdbc/ds1");
        ... update the database and get next item to process
    }
}, Runnable.class);
barrier = new CyclicBarrier(3, updateAndGetNextFromDatabase);
...
```

## Configuring managed scheduled executors

8.5.5.4

You can configure `ManagedScheduledExecutorService` instances to schedule asynchronous tasks to run with the thread context of the thread from which the task is scheduled. It is a best practice for Java EE applications to avoid directly managing their own threads; therefore, the `ManagedScheduledExecutorService` extends the JSE `ExecutorService` to provide a way to schedule asynchronous tasks within an application server environment. You might also configure the `ManagedScheduledExecutorService` to capture a thread context that is relevant to Java EE applications and propagate it to the thread of the scheduled task.

## About this task

**Important:** In Liberty, managed scheduled executors do not have their own thread pools. Tasks submitted to managed scheduled executor instances run on the common Liberty executor thread pool.

The managed scheduled executor `<concurrent-1.0>` feature is enabled in the `server.xml` file as follows:

```
<featureManager>
  <feature>concurrent-1.0</feature>
</featureManager>
```

Thread context capture and propagation is managed by the context service. A default instance of the context service (`DefaultContextService`) is created by the server and configured to propagate at least `classloaderContext`, `jeeMetadataContext` and `securityContext`. This default context service instance is used if a `ManagedScheduledExecutorService` is created without referring to a specific context service instance or configuring a context service instance directly within. For more information about context service instances, refer to the [Configuring thread context service instances](#) topic.

A default managed scheduled executor instance (`DefaultManagedScheduledExecutorService`) is available as `java:comp/DefaultManagedScheduledExecutorService` and uses the default context service instance for thread context capture and propagation.

## Procedure

Example configuration in the `server.xml` file:

- Managed scheduled executor that is registered in JNDI with the name `concurrent/scheduledExecutor`, and that uses the default context service instance:

```
<managedScheduledExecutorService jndiName="concurrent/scheduledExecutor"/>
```

- Managed scheduled executor with context service configured to capture and propagate `classloaderContext` only:

```
<managedScheduledExecutorService jndiName="concurrent/scheduledExecutor1">
  <contextService>
    <classloaderContext/>
  </contextService>
</managedScheduledExecutorService>
```

- Managed scheduled executor with `jeeMetadataContext` and `securityContext`:

```
<managedScheduledExecutorService jndiName="concurrent/scheduledExecutor2">
  <contextService>
    <jeeMetadataContext/>
    <securityContext/>
  </contextService>
</managedScheduledExecutorService>
```

- Thread context service that is shared by multiple managed scheduled executors:

```
<contextService id="contextSvc1">
  <jeeMetadataContext/>
</contextService>
```

```
<managedScheduledExecutorService jndiName="concurrent/scheduledExecutor3"
contextServiceRef="contextSvc1"/>
```

```
<managedScheduledExecutorService jndiName="concurrent/scheduledExecutor4" contextServiceRef="contextSvc1"/>
```

## Example

Inject managed scheduled executors into application components (by using `@Resource`) or look up with resource environment references (`resource-env-ref`). Regardless of how the instance is obtained, it can be

used interchangeably as `javax.enterprise.concurrent.ManagedScheduledExecutorService` or any of the following superclasses: `java.util.concurrent.ScheduledExecutorService`, `java.util.concurrent.ExecutorService`, `javax.enterprise.concurrent.ManagedExecutorService`

- Example that looks up the default managed scheduled executor:

```
ManagedScheduledExecutorService executor =
    (ManagedScheduledExecutorService) new InitialContext().lookup(
        "java:comp/DefaultManagedScheduledExecutorService");
executor.schedule(beginSalePrices, 12, TimeUnit.HOURS);
executor.schedule(restoreNormalPrices, 60, TimeUnit.HOURS);
```

- Example that uses `@Resource` to inject as `java.util.concurrent.ScheduledExecutorService`:

```
@Resource(lookup="concurrent/scheduledExecutor2")
ScheduledExecutorService executor;
...

// schedule a task to run every half hour from now
Runnable updateSalesReport = new Runnable() {
    public void run() throws Exception {
        // java:comp lookup is possible because <jeeMetadataContext> is configured
        DataSource ds = (DataSource) new InitialContext().lookup("java:comp/env/jdbc/ds1");
        ... query and update various database tables
    }
};
ScheduledFuture<?> future = executor.scheduleAtFixedRate(updateSalesReport, 0, 30, TimeUnit.MINUTES);
```

- Example that uses `@Resource` to inject as `javax.enterprise.concurrent.ManagedScheduledExecutorService`:

```
@Resource(lookup="concurrent/scheduledExecutor2")
ManagedScheduledExecutorService executor;
```

... usage is same as previous example

- Example `<resource-env-ref>` for `java.util.concurrent.ScheduledExecutorService` in the `web.xml` file:

```
<resource-env-ref>
  <resource-env-ref-name>concurrent/scheduledExecutor1</resource-env-ref-name>
  <resource-env-ref-type>java.util.concurrent.ScheduledExecutorService</resource-env-ref-type>
</resource-env-ref>
```

- Example `<resource-env-ref>` for `javax.enterprise.concurrent.ManagedScheduledExecutorService` in the `web.xml` file:

```
<resource-env-ref>
  <resource-env-ref-name>concurrent/scheduledExecutor2</resource-env-ref-name>
  <resource-env-ref-type>javax.enterprise.concurrent.ManagedScheduledExecutorService</resource-env-ref-type>
</resource-env-ref>
```

- Example lookup that uses a resource environment reference:

```
ManagedScheduledExecutorService executor =
    (ManagedScheduledExecutorService) new InitialContext().lookup("java:comp/env/concurrent/scheduledExecutor2");
executor.schedule(payrollTask, fridaysAtMidnightTrigger);
```

## Configuring managed thread factories

8.5.5.4

You can configure `ManagedThreadFactory` instances to create new threads that run with a thread context of the thread from which the managed thread factory is looked up or injected. It is a best practice for Java EE applications to avoid directly managing their own threads; therefore, the `ManagedThreadFactory` extends the JSE `ThreadFactory` to provide a way to create managed threads within an application server environment. You might also configure the `ManagedThreadFactory` to capture a thread context that is relevant to Java EE applications and propagate it to the new thread.

### About this task

The managed thread factory is available under the `<concurrent-1.0>` feature and enabled in the `server.xml` file as follows:

```
<featureManager>
  <feature>concurrent-1.0</feature>
</featureManager>
```

Thread context capture and propagation is managed by the context service. A default instance of the context service (`DefaultContextService`) is created by the server and configured to propagate at least `classloaderContext`, `jeeMetadataContext` and `securityContext`. This default context service instance is used if a `ManagedThreadFactory` does not specify a context service. For more information about context service instances, refer to the [Configuring thread context service instances](#) topic.

A default instance of `ManagedThreadFactory` (`DefaultManagedThreadFactory`) is available as `java:comp/DefaultManagedThreadFactory` and uses the default context service instance for thread context capture and propagation.

## Procedure

Example configuration in the `server.xml` file:

- Managed thread factory that is registered in JNDI with the name `concurrent/threadFactory`, and that uses the default context service instance:

```
<managedThreadFactory jndiName="concurrent/threadFactory" maxPriority="5"/>
```

- Managed thread factory with context service configured to capture and propagate `securityContext` only:

```
<managedThreadFactory jndiName="concurrent/threadFactory1">
  <contextService>
    <securityContext/>
  </contextService>
</managedThreadFactory>
```

- Managed thread factory with `classloaderContext` and `jeeMetadataContext`:

```
<managedThreadFactory jndiName="concurrent/threadFactory2">
  <contextService>
    <classloaderContext/>
    <jeeMetadataContext/>
  </contextService>
</managedThreadFactory>
```

- Thread context service that is shared by multiple managed thread factories:

```
<contextService id="contextSvc1">
  <jeeMetadataContext/>
</contextService>
```

```
<managedThreadFactory jndiName="concurrent/threadFactory3"
contextServiceRef="contextSvc1"/>
```

```
<managedThreadFactory jndiName="concurrent/threadFactory4"
contextServiceRef="contextSvc1"/>
```

## Example

Managed thread factories can be injected into application components (by using `@Resource`) or looked up with resource environment references (`resource-env-ref`). Regardless of how the instance is obtained, it can be used interchangeably as `javax.enterprise.concurrent.ManagedThreadFactory` or `java.util.concurrent.ThreadFactory`.

- Example that looks up the default managed thread factory:

```
ManagedThreadFactory threadFactory =
    (ManagedThreadFactory) new InitialContext().lookup(
        "java:comp/DefaultManagedThreadFactory");
```

```
// Create an executor that always runs tasks with the thread context of the managed thread factory
ExecutorService executor = new ThreadPoolExecutor(
    coreThreads, maxThreads, keepAliveTime, TimeUnit.MINUTES,
    new ArrayBlockingQueue<Runnable>(workRequestQueueSize),
    threadFactory, new ThreadPoolExecutor.AbortPolicy());
```

- Example that uses `@Resource` to inject `asjava.util.concurrent.ThreadFactory`:

```
@Resource(lookup="concurrent/threadFactory2")
ThreadFactory threadFactory
...
```

```
// create a new thread
Thread dailySalesAnalysisTask = threadFactory.newThread(new Runnable() {
    public void run() {
        // java:comp lookup is possible because <jeeMetadataContext> is configured
        DataSource ds = (DataSource) new InitialContext().lookup("java:comp/env/jdbc/ds1");
        ... analyze the data
    }
});
dailySalesAnalysisTask.start();
```

- Example that uses `@Resource` to inject as `javax.enterprise.concurrent.ManagedThreadFactory`:

```
@Resource(lookup="concurrent/threadFactory2")
ManagedThreadFactory threadFactory;
```

... usage is same as previous example

- Example `<resource-env-ref>` for `java.util.concurrent.ThreadFactory` in the `web.xml` file:

```
<resource-env-ref>
  <resource-env-ref-name>concurrent/threadFactory1</resource-env-ref-name>
  <resource-env-ref-type>java.util.concurrent.ThreadFactory</resource-env-ref-type>
</resource-env-ref>
```

- Example `<resource-env-ref>` for `javax.enterprise.concurrent.ManagedThreadFactory` in the `web.xml` file:

```
<resource-env-ref>
  <resource-env-ref-name>concurrent/threadFactory2</resource-env-ref-name>
  <resource-env-ref-type>javax.enterprise.concurrent.ManagedThreadFactory</resource-
env-ref-type>
</resource-env-ref>
```

- Example lookup that uses a resource environment reference:

```
ManagedThreadFactory threadFactory =
    (ManagedThreadFactory) new InitialContext().lookup("java:comp/env/concurrent/threadFactory");
// Create a scheduled executor that always runs tasks with the thread context of the managed thread factory
ScheduledExecutorService executor = Executors.newScheduledThreadPool(5, threadFactory);
... use executor to schedule tasks from any thread
```

## Connecting to Liberty by using JMX

Use this information to access Java Management Extensions (JMX) connectors on Liberty. You can also access the secured JMX connector remotely by using SSL.

### About this task

There are two JMX connectors supported on Liberty, each connector is enabled through a different Liberty feature: `localConnector-1.0` and `restConnector-1.0`.

- The local connector is enabled through the Liberty feature `localConnector-1.0`. Access through the local connector is protected by the policy implemented by the SDK in use. Currently the SDKs require that the client runs on the same host as Liberty, and under the same user ID.
- The REST connector is enabled through the Liberty feature `restConnector-1.0`. Remote access through the REST connector is protected by a single administrator role. In addition, SSL is required to keep the communication confidential. The `restConnector-1.0` feature already includes the `ssl-1.0` feature.

An application deployed on Liberty has unrestricted access to its MBeanServer directory.

A JMX connection to the collective controller enables JMX access to multiple Liberty servers through the same connection. See “Setting up the server-management environment for Liberty by using collectives” on page 1134 for more information.

**Restriction:** Do not use JDK options that start with `com.sun.management.jmxremote`, which are described in <http://docs.oracle.com/javase/7/docs/technotes/guides/management/agent.html>, with the Liberty JMX support. Those JDK options adversely affect the Liberty MBean registration framework.

## Procedure

- Connect to the local JMX connector
- Connect to the REST connector
- **8.5.0.1** Work with JMX MBeans

## Configuring local JMX connection to Liberty

You can access the local Java Management Extensions (JMX) connector on Liberty. The local connector is enabled through the Liberty feature `localConnector-1.0`.

### About this task

The local connector is enabled through the Liberty feature `localConnector-1.0`. Access through the local connector is protected by the policy implemented by the SDK in use. Currently the SDKs require that the client runs on the same host as Liberty, and under the same user ID.

**Note:** An application deployed on Liberty has unrestricted access to its MBeanServer directory.

The following section describes how to configure and access the local connector on Liberty.

## Procedure

1. Enable the local connector by using the following code in the `server.xml` file.

```
<featureManager>
  <feature>localConnector-1.0</feature>
</featureManager>
```
2. **8.5.0.1** Access the local connector by using the JConsole tool or JMX client that is installed on the same host.
  - For the JConsole tool, select the local process `ws-server.jar defaultServer` from the connection panel then click **Connect**.
  - **8.5.0.1** For the JMX client, see “Working with JMX MBeans on Liberty” on page 1646.

## Configuring secure JMX connection to Liberty

You can access the secured Java Management Extensions (JMX) connectors on Liberty by using SSL. The secured JMX connection is enabled by the Liberty feature `restConnector-1.0`.

### About this task

The REST connector is enabled through the Liberty feature `restConnector-1.0`. Remote access through the REST connector is protected by a single administrator role. In addition, SSL is required to keep the communication confidential. The `restConnector-1.0` feature already includes the `ssl-1.0` feature.

**Note:** An application deployed on Liberty has unrestricted access to its MBeanServer directory.

The following section describes how to configure and access the REST connector on Liberty.

## Procedure

1. Enable the REST connector using the following code in the `server.xml` file.

```
<featureManager>
  <feature>restConnector-1.0</feature>
</featureManager>
```

2. Configure SSL certificates in the `server.xml` file.

Ensure that the CN value of the certificate's subjectDN is the host name of the machine where the server is running, and that the truststore contains the certificate of the server in the jConsole connection.

3. Configure a user or group to the administrator role in the `server.xml` file.

- Map to the administrator role for Liberty
- **z/OS** Map to the administrator role for Liberty on z/OS

4. Access the REST connector.

**8.5.5.4** You can access a Liberty REST connector from a Java client or directly through an HTTPS call. A Java client uses the client-side of the connector, which is in `wlp/clients/restConnector.jar` and implements the `javax.management.MBeanServerConnection` interface. HTTPS calls use the server-side of the connector. As to HTTPS calls on the server-side, any programming language that can make HTTPS calls, such as C++, JavaScript, curl, Ruby, and Perl, can use the REST APIs. The REST APIs contain endpoints for management (JMX), file transfer, collective routing and collective deployment.

- Access the REST connector from a JMX client application or by using the jConsole tool provided in the Java SDK. Use `-J` flags to pass the system properties as Java options and set the class path to include the connector class files. The connector class files are packed in the `clients/restConnector.jar` file.

- Use the following properties for SSL certificates:

```
-J-Djavax.net.ssl.trustStore=<location of your client trust store>
-J-Djavax.net.ssl.trustStorePassword=<password for the trust store>
-J-Djavax.net.ssl.trustStoreType=<type of trust store>
```

The following example shows the jConsole tool being used with SSL configurations:

```
jconsole -J-Djava.class.path=%JAVA_HOME%/lib/jconsole.jar;
          %JAVA_HOME%/lib/tools.jar;
          %WLP_HOME%/clients/restConnector.jar
          -J-Djavax.net.ssl.trustStore=key.jks
          -J-Djavax.net.ssl.trustStorePassword=Liberty
          -J-Djavax.net.ssl.trustStoreType=jks
```

After the jConsole starts, select **Remote Process**, and enter the JMX service URL: `service:jmx:rest://<host>:<port>/IBMJMXConnectorREST`. The port number is the HTTPS port. You must also provide the user name and password.

- **z/OS** For z/OS, use the following system properties:

```
-J-Djava.protocol.handler.pkgs=com.ibm.crypto.provider
-J-Djavax.net.ssl.trustStore=<SAF keyring>
-J-Djavax.net.ssl.trustStorePassword=<password to SAF>
-J-Djavax.net.ssl.trustStoreType=JCERACFKS
```

- **8.5.5.4** Access the REST connector directly using an HTTPS call.

To use HTTPS calls to access REST connectors, you need WebSphere Application Server Liberty 8.5.5.4 or later.

- a. Open a browser at `https://<host>:<port>/IBMJMXConnectorREST/api`, and enter the administrative credentials you specified in step 3.
- b. Examine the available REST APIs. Each item has a description of its behavior, input, output, query parameters, and header.

**Note:** You can specify some JMX REST connection options as system properties. See the Liberty API - WebSphere JMX REST Connector API.

## Mapping the administrator role for Liberty:

You can use `quickStartSecurity` element or any supported user registries for the administrator role mapping in Liberty.

### About this task

All the JMX methods and MBeans accessed through the REST connector are currently protected by a single role named "administrator". To get started quickly, use `quickStartSecurity` element to configure a single user with administrator role and configure the default SSL configuration.

You can also use any supported user registry. You cannot use `quickStartSecurity` element if you have already configured another user registry. In this case, you have to map users or roles from the registry to the administrator role.

### Procedure

- Use `quickStartSecurity` element for a single user mapping.

Here is an example showing the minimal required configuration:

```
<featureManager>
  <feature>restConnector-1.0</feature>
</featureManager>
<quickStartSecurity userName="bob" userPassword="bobpassword" />
<keyStore id="defaultKeyStore" password="keystorePassword"/>
```

- Or use the basic registry for administrator role mapping.

Here is an example of the basic registry that gives the user "bob" or the group "group1" administrator role:

```
<basicRegistry>
  <user name="bob" password="bobpassword"/>
  <user name="joe" password="joepassword"/>
  <group name="group1" ...>
  </group>
</basicRegistry>

<administrator-role>
  <user>bob</user>
  <group>group1</group>
</administrator-role>
```

- Or use the LDAP registry for administrator role mapping **8.5.5.0** (you will need to add the `ldapRegistry-3.0` feature to your `server.xml` file).

Here is an example of the LDAP registry that gives the user "bob" administrator role.

```
<ldapRegistry id="basic" host="" port="">
  <tds.properties ... />
</ldapRegistry>

<administrator-role>
  <user>cn=bob,o=ibm,c=us</user>
</administrator-role>
```

## Mapping the administrator role for Liberty on z/OS: **z/OS**

You must configure SAF keyring and RACF authorization to map a z/OS user to an administrator role for Liberty on z/OS.

## About this task

For z/OS users using SAF keyring and RACF authorization, the SSL definition must point to SAF, and the administrator role is defined in RACF.

## Procedure

- Configure SSL definitions with SAF. Here is a sample configuration:

```
<featureManager>
  <feature>zosSecurity-1.0</feature>
  <feature>restConnector-1.0</feature>
</featureManager>

<sslDefault sslRef="defaultSSLSettings" />
<ssl id="defaultSSLSettings" keyStoreRef="CellDefaultKeyStore"
  trustStoreRef="CellDefaultTrustStore" />
<keyStore id="CellDefaultKeyStore" location="safkeyring:///WASKeyring2048" type="JCERACFKS"
  password="keystorepassword" fileBased="false" readOnly="true" />
<keyStore id="CellDefaultTrustStore" location="safkeyring:///WASKeyring2048" type="JCERACFKS"
  password="truststorepassword" fileBased="false" readOnly="true" />
```

- Configure administrator role by using RACF authorization.

To assign a user to the administrator role, you must grant the user access to the SAF profile associated with the role. See “Liberty: Controlling how roles are mapped to SAF Profiles” on page 1941 for more details.

By default, the SAF profile name for the administrator role is `BBGZDFLT.com.ibm.ws.management.security.resource.Administrator`. That profile must exist in the `EJBROLE` SAF class, and the admin user must be granted `READ` access to it.

Here is the example RACF commands for user `mstone1`:

```
RDEFINE EJBROLE BBGZDFLT.com.ibm.ws.management.security.resource.Administrator UACC(NONE)
PERMIT BBGZDFLT.com.ibm.ws.management.security.resource.Administrator ID(MSTONE1) ACCESS(READ) CLASS(EJBROLE)
```

## Developing a JMX Java client for Liberty:

You can develop a Java Management Extensions (JMX) client application to access the secured REST connector of the Liberty server.

## About this task

Using a JMX remote client application, you can administer the Liberty server through JMX programming.

## Procedure

- Develop a sample JMX client as follows. The REST connector supports the standard JMX API.

```
import javax.management.remote.JMXServiceURL;
import javax.management.MBeanServerConnection;
import javax.management.remote.JMXConnector;
import javax.management.remote.JMXConnectorFactory;
import java.util.HashMap;

public class Test {

    public static void main(String[] args) {
        System.setProperty("javax.net.ssl.trustStore", <truststore location>);
        System.setProperty("javax.net.ssl.trustStorePassword", <truststore password>);

        //If the type of the trustStore is not jks, which is default,
        //set the type by using the following line.
        System.setProperty("javax.net.ssl.trustStoreType", <truststore type>);
```

```

try {
    HashMap<String, Object> environment = new HashMap<String, Object>();
    environment.put("jmx.remote.protocol.provider.pkgs", "com.ibm.ws.jmx.connector.client");
    environment.put(JMXConnector.CREDENTIALS, new String[] { "bob", "bobpassword" });

    JMXServiceURL url = new JMXServiceURL("service:jmx:rest://<host>:<port>/IBMJMXConnectorREST");
    JMXConnector connector = JMXConnectorFactory.newJMXConnector(url, environment);
    connector.connect();
    MBeanServerConnection mbsc = connector.getMBeanServerConnection();
} catch(Throwable t) {
    ...
}
}
}

```

- Optional: Disable host name verification for SSL certificates. The certificates that are installed with the Liberty profile might not contain the host name of where the server is actually running. If you want to disable host name verification of SSL certificates, you can set the system property `com.ibm.ws.jmx.connector.client.disableURLHostnameVerification` to `true`, which disables host name verification for all connections. To disable host name verification on a per-connection basis, pass the property as a new environment when you create the JMX connection:

```

HashMap<String, Object> environment = new HashMap<String, Object>();
environment.put("jmx.remote.protocol.provider.pkgs", "com.ibm.ws.jmx.connector.client");
environment.put("com.ibm.ws.jmx.connector.client.disableURLHostnameVerification", Boolean.TRUE);
environment.put(JMXConnector.CREDENTIALS, new String[] { "bob", "bobpassword" });
...

```

- Optional: Configure JMX REST connector settings by using the environment Map.

```

...
HashMap<String, Object> environment = new HashMap<String, Object>();
environment.put("com.ibm.ws.jmx.connector.client.rest.maxServerWaitTime", 0);
environment.put("com.ibm.ws.jmx.connector.client.rest.notificationDeliveryInterval", 65000);
...

```

- **8.5.5.0** Optional: The Liberty REST connector allows you to specify a custom SSL socket factory that can be used to obtain sockets. If the `javax.net.ssl.SSLHandshakeException`: `com.ibm.jsse2.util.j: PKIX path building failed: java.security.cert.CertPathBuilderException: unable to find valid certification path to requested target` exception is displayed, you can create your own `SSLContext` from your own `KeyStores` and then use the `SocketFactory` from that context with the REST connector.

```

KeyStore trustStore = KeyStore.getInstance(KeyStore.getDefaultType());
InputStream inputStream = new FileInputStream("myTrustStore.jks");
trustStore.load(inputStream, "password".toCharArray());
TrustManagerFactory trustManagerFactory = TrustManagerFactory.getInstance(TrustManagerFactory.getDefaultAlgorithm());
trustManagerFactory.init(trustStore);
TrustManager[] trustManagers = trustManagerFactory.getTrustManagers();
SSLContext sslContext = SSLContext.getInstance("SSL");
sslContext.init(null, trustManagers, null);

```

```

Map<String, Object> environment = new HashMap<String, Object>();
environment.put(ConnectorSettings.CUSTOM_SSLSOCKETFACTORY, sslContext.getSocketFactory());
environment.put(ConnectorSettings.DISABLE_HOSTNAME_VERIFICATION, true);
environment.put("jmx.remote.protocol.provider.pkgs", "com.ibm.ws.jmx.connector.client");
environment.put(JMXConnector.CREDENTIALS, new String[] { "admin", "password" });
JMXServiceURL url = new JMXServiceURL("REST", "myhost", 9443, "/IBMJMXConnectorREST");
jmxConn = JMXConnectorFactory.connect(url, environment);

```

## Working with JMX MBeans on Liberty

### 8.5.0.1

You can access the attributes and call the operations of Java Management Extensions (JMX) management beans (MBeans) on Liberty. In addition, you can register your own MBeans from an application running on Liberty.

## About this task

The primary interfaces for interacting with MBeans on Liberty are as follows:

- `javax.management.MBeanServer`, which is for application code running on Liberty.
- `javax.management.MBeanServerConnection`, which is for external code running in a separate Java virtual machine.

You can use an instance of either of these interfaces to access the attributes and call the operations of MBeans.

## Procedure

- For application code running on Liberty, you can use a `javax.management.MBeanServer` instance by using the following code:

```
import java.lang.management.ManagementFactory;
import javax.management.MBeanServer;

...

MBeanServer mbs = ManagementFactory.getPlatformMBeanServer();
...
```

- For external code running in a separate Java virtual machine, you can use a `javax.management.MBeanServerConnection` instance. See “Developing a JMX Java client for Liberty” on page 1645.

## Liberty: List of provided MBeans: **8.5.0.1**

Liberty provides a list of MBeans and corresponding management interfaces that you can use to manipulate and monitor the server.

For each MBean or MXBean in the list:

- The name is the `javax.management.ObjectName` value that uniquely identifies the MBean or MXBean. When there are multiple instances of an MBean or MXBean, the `ObjectName` value can contain a wildcard (\*), which is described in the **Comments** entries in this topic.
- The **Management interface** entries specify the name of the Java interface that can be used to construct a proxy object for the MBean or MXBean as described in “Liberty:Examples of accessing MBean attributes and operations” on page 1654. For more information about the management interface, see the Java API document for Liberty. The Java API documentation for each Liberty API is available in a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

### **8.5.5.0**

**WebSphere: feature=channel fw, type=endpoint, name=\***

- **Management interface:** `com.ibm.websphere.endpoint.EndPointInfoMBean`
- **Comments:** One instance is available for each endpoint in the system, where \* is a unique endpoint name.

### **8.5.5.0**

**WebSphere: feature=clusterMember, type=ClusterMember, name=ClusterMember**

- **Management interface:** `com.ibm.websphere.cluster.member.ClusterMemberMBean`

- **Comments:** This MBean is available when the `clusterMember` feature is enabled on a collective member. To join a cluster, add `<clusterMember name=<clusterName> />` into the server configuration. The name of the cluster can be retrieved by this MBean.

#### 8.5.5.0

**WebSphere: feature=collectiveController, type=ClusterManager, name=ClusterManager**

- **Management interface:** `com.ibm.websphere.collective.controller.ClusterManagerMBean`
- **Comments:** This MBean is available when the `collectiveController` feature is enabled. It provides operations that can be used to query and manipulate Liberty servers that have enabled the `collectiveMember` and `clusterMember` features.

#### 8.5.5.5

**WebSphere: feature=collectiveController, type=AdminMetadataManager, name=AdminMetadataManager**

- **Management interface:** `com.ibm.websphere.collective.repository.AdminMetadataManagerMBean`
- **Comments:** This MBean provides the administrative metadata MBean operations to add, retrieve and remove metadata. The metadata includes tags, owner, contact, and note data. The metadata information is stored in the collective repository. You can find the MBean class and API documentation in the following locations:
  - `${wlp.install.dir}/dev/api/ibm/com.ibm.websphere.appserver.api.collectiveController_version.jar`
  - `${wlp.install.dir}/dev/api/ibm/javadoc/com.ibm.websphere.appserver.api.collectiveController_version-javadoc.zip`

#### 8.5.5.0

**WebSphere: feature=collectiveController, type=CollectiveRegistration, name=CollectiveRegistration**

- **Management interface:** `com.ibm.websphere.collective.controller.CollectiveRegistrationMBean`
- **Comments:** This MBean is available when the `collectiveController` feature is enabled. It provides operations that enable registration of hosts, Liberty servers to be joined as members, replication of new controllers, and controller access authentication of members to the collective controller.

#### 8.5.5.0

**WebSphere: feature=collectiveController, type=CollectiveRepository, name=CollectiveRepository**

- **Management interface:** `com.ibm.websphere.collective.repository.CollectiveRepositoryMBean`
- **Comments:** This MBean is available when the `collectiveController` feature is enabled. It provides operations that enable reading and writing of data into the collective repository.

#### 8.5.5.0

**WebSphere: feature=collectiveController, type=RepositoryConfiguration, name=RepositoryConfiguration**

- **Management interface:** `com.ibm.websphere.collective.repository.RepositoryConfigurationMBean`
- **Comments:** This MBean is available when the `collectiveController` feature is enabled. It provides operations that enable adding and removing collective controller replicas to scale out the replica set and provide high availability capabilities.

#### 8.5.5.0

**WebSphere: feature=collectiveController, type=RepositoryPathUtility, name=RepositoryPathUtility**

- **Management interface:** `com.ibm.websphere.collective.repository.RepositoryPathUtilityMBean`
- **Comments:** This MBean is available when the `collectiveController` feature is enabled. It provides utility operations that enable easier construction of paths for use with the `RepositoryConfiguration` MBean.

### 8.5.5.0

**WebSphere: feature=collectiveController, type=RoutingContext, name=RoutingContext**

- **Management interface:**com.ibm.websphere.collective.controller.RoutingContextMBean
- **Comments:** This MBean is for setting up the JMX routing context - to call MBeans on a collective member server through a collective controller for example.

**Note:** **Distributed operating systems** **IBM i** The collectiveController-1.0 feature and its capabilities are available only in WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. The feature is not available in WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a WebSphere Application Server Liberty Network Deployment installation, you can use its collectiveController-1.0 feature to work with collective members from WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core installations.

See “Liberty: Example of setting up a JMX routing environment” on page 1657 for more information.

### 8.5.5.0

**WebSphere: feature=collectiveController, type=ServerCommands, name=ServerCommands**

- **Management interface:**com.ibm.websphere.collective.controller.ServerCommandsMBean
- **Comments:** This MBean runs in the collective controller and can remotely invoke the Liberty **server** command on a target host. It has three operations: `getServerStatus`, `startServer`, and `stopServer`. The `getServerStatus` operation allows you to get the status of a member server in a collective by providing its hostname, server's user directory, and server name. You can subscribe for server up or down changes by calling `addNotificationListener`. An `AttributeChangeNotification` is sent to all listeners when any server in the collective changes its state. The hostname, server's user directory, and server name are stored as a comma-separated string in the message for identification purposes.

You can find the MBean class and API documentation in the following locations:

- `${wlp.install.dir}/dev/api/ibm/com.ibm.websphere.appserver.api.collectiveController_version.jar`
- `${wlp.install.dir}/dev/api/ibm/javadoc/com.ibm.websphere.appserver.api.collectiveController_version-javadoc.zip`

**Note:** **Distributed operating systems** **IBM i** The collectiveController-1.0 feature and its capabilities are available only in WebSphere Application Server Liberty Network Deployment and WebSphere Application Server Liberty for z/OS. **8.5.5.0** The feature is not available in WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a WebSphere Application Server Liberty Network Deployment installation, you can use its collectiveController-1.0 feature to work with collective members from WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core installations.

### 8.5.5.0

**WebSphere: feature=restConnector, type=FileService, name=FileService**

- **Management interface:**com.ibm.websphere.filetransfer.FileServiceMXBean
- **Comments:** This MXBean enables you to perform various file-related operations on the host where Liberty resides.

You can find its class and API documentation in the following locations:

- `liberty_home/dev/api/ibm/com.ibm.websphere.appserver.api.restConnector_version.jar`
- `liberty_home/dev/api/ibm/javadoc/com.ibm.websphere.appserver.api.restConnector_version-javadoc.zip`

The exposed operations include the ability to query certain metadata (last modified date, size, and so on) for a given file or directory and also to query all child files (and corresponding metadata) for a given directory. Support for archive creation and expansion is also provided, which can be useful to compress Liberty log files or to extract an application before deploying it.

This MBean contains two attributes: the read list and the write list. They represent the lists of locations that users can read or write to when using the FileService or FileTransfer capabilities provided by Liberty. Through the MBean, these attributes can only be read, but they can be configured or customized through the following elements in the `server.xml` file:

```
<remoteFileAccess>
  <readDir>${server.output.dir}/logs</readDir>
  <readDir>${server.output.dir}/apps</readDir>
  <writeDir>${server.output.dir}/dropins</writeDir>
</remoteFileAccess>
```

If the `readDir` element is not specified, the default is the combination of: `${wlp.install.dir}`, `${wlp.user.dir}`, and `${server.output.dir}`. If a `writeDir` element is not specified, the default is the empty set.

The `restConnector-1.0` feature must be included in the `server.xml` file in order for this MBean to be loaded and to honor its configuration elements

Using Liberty-defined variables is allowed with all the server-side parameters that take a string representing a file path. Such variables are defined on the `liberty_home/README.TXT` file.

#### 8.5.5.0

##### **WebSphere: feature=restConnector, type=FileTransfer, name=FileTransfer**

- **Management interface:** `com.ibm.websphere.filetransfer.FileTransferMBean`
- **Comments:** This MBean allows you to perform various file-transfer operations on the host where Liberty resides.

You can find its class and API documentation in the following locations:

```
liberty_home/dev/api/ibm/com.ibm.websphere.appserver.api.restConnector_version.jar
liberty_home/dev/api/ibm/javadoc/com.ibm.websphere.appserver.api.restConnector_version-javadoc.zip
```

This MBean is registered on the PlatformMBeanServer from the same JVM that its corresponding Liberty process is running, but it can be accessed only by using the IBM JMX REST Connector. The connection can be local or remote, but the REST Connector must be used.

The exposed operations include the ability to download, upload, and delete a file. Each read and write request on the server is bound to the configurable read and write lists that are accessed through the FileServiceMBean. The FileTransferMBean can also be fully accessed and operated from the built-in Java JConsole, provided that the JConsole is connected through the IBM JMX REST Connector.

Using Liberty-defined variables is allowed with all the server-side parameters that take a string representing a file path. Such variables are defined on the `liberty_home/README.TXT` file.

#### 8.5.5.5

##### **WebSphere: name=com.ibm.websphere.config.mbeans.ServerXMLConfigurationMBean**

- **Management interface:** `com.ibm.websphere.config.mbeans.ServerXMLConfigurationMBean`
- **Comments:** The ServerXMLConfigurationMBean provides an interface for retrieving the file paths of all server configuration files known to the server. The MBean is available from the Kernel, so you do not need to enable a special feature. You can find the MBean class and API documentation in the following locations:
  - `${wlp.install.dir}/dev/api/ibm/com.ibm.websphere.appserver.api.config_version.jar`
  - `${wlp.install.dir}/dev/api/ibm/javadoc/com.ibm.websphere.appserver.api.config_version-javadoc.zip`

#### 8.5.5.4

**WebSphere:name=com.ibm.websphere.runtime.update.RuntimeUpdateNotificationMBean**

- **Management interface:**com.ibm.websphere.runtime.update.RuntimeUpdateNotificationMBean
- **Comments:** The RuntimeUpdateNotificationMBean provides notifications for server runtime updates. The user data object attached to the notification is a java.util.Map. The notification type for runtime update notifications emitted by this MBean is com.ibm.websphere.runtime.update.notification.

8.5.5.5

**WebSphere:name=com.ibm.ws.config.mbeans.FeatureListMBean**

- **Management interface:**com.ibm.websphere.config.mbeans.FeatureListMBean
- **Comments:** The FeatureListMBean exposes a single method to generate an XML report on all the features installed at run time. The MBean is available from the Kernel, so you do not need to enable a special feature. You can find the MBean class and API documentation in the following locations:
  - `${wlp.install.dir}/dev/api/ibm/com.ibm.websphere.appserver.api.config_version.jar`
  - `${wlp.install.dir}/dev/api/ibm/javadoc/com.ibm.websphere.appserver.api.config_version-javadoc.zip`

8.5.5.5

**WebSphere:name=com.ibm.ws.config.serverSchemaGenerator**

- **Management interface:**com.ibm.websphere.config.mbeans.ServerSchemaGenerator
- **Comments:** The ServerSchemaGenerator MBean exposes methods to generate schema from the installed image, the most used way, or from a current runtime. The MBean is available from the Kernel, so you do not need to enable a special feature. You can find the MBean class and API documentation in the following locations:
  - `${wlp.install.dir}/dev/api/ibm/com.ibm.websphere.appserver.api.config_version.jar`
  - `${wlp.install.dir}/dev/api/ibm/javadoc/com.ibm.websphere.appserver.api.config_version-javadoc.zip`

**WebSphere:name=com.ibm.ws.jmx.mbeans.generatePluginConfig**

- **Management interface:**com.ibm.websphere.webcontainer.GeneratePluginConfigMBean
- **Comments:** See “Configuring a web server plug-in for Liberty” on page 1604.

**WebSphere:service=com.ibm.ws.kernel.filemonitor.FileNotificationMBean**

- **Management interface:**com.ibm.websphere.filemonitor.FileNotificationMBean

**WebSphere:service=com.ibm.websphere.application.ApplicationMBean,name=\***

- **Management interface:**com.ibm.websphere.application.ApplicationMBean
- **Comments:** One instance is available for each application in the system, where \* is a unique application name.

8.5.5.6

**WebSphere:service=com.ibm.ws.jca.cm.mbean.ConnectionManagerMBean,\***

- **Management interface:**com.ibm.ws.jca.cm.mbean.ConnectionManagerMBean
- **Comments:** One instance is available for each Connection Manager in the system, including those created in the following contexts:
  - When explicitly configured in the server configuration
  - When implicitly created because of @DataSourceDefinition or @ConnectionFactoryDefinition annotations
  - When created as a result of a connection factory or data source in the server configuration

The mbean instance is not available until the corresponding connection factory or data source is first used.

To narrow the connection manager instance, you can specify additional attributes, such as those shown in the following examples:

```
WebSphere:service=com.ibm.ws.jca.cm.mbean.ConnectionManagerMBean,jndiName=jdbc/db2,*
```

```
WebSphere:service=com.ibm.ws.jca.cm.mbean.ConnectionManagerMBean,name=jmsConnectionFactory[cf1]/connectionManager[default]
```

```
WebSphere:service=com.ibm.ws.jca.cm.mbean.ConnectionManagerMBean,name=databaseStore[dbstore1]/dataSource[default-0]/conn
```

```
WebSphere:service=com.ibm.ws.jca.cm.mbean.ConnectionManagerMBean,jndiName=java.module/env/jdbc/ds3,application=MyApp,modu
```

#### **WebSphere:type=JvmStats**

- **Management interface:** com.ibm.websphere.monitor.jmx.JvmMXBean
- **Comments:** Available when the monitor-1.0 feature is enabled. See “Liberty:JVM monitoring” on page 2267.

#### **WebSphere:type=ServletStats,name=\***

- **Management interface:**com.ibm.websphere.webcontainer.ServletStatsMXBean
- **Comments:** When the monitor-1.0 feature is enabled, one instance is available for each servlet that has been served, where \* is of the form <AppName>.<ServletName>. See “Liberty:Web application monitoring” on page 2268.

#### **WebSphere:type=ThreadPoolStats,name=Default Executor**

- **Management interface:**com.ibm.websphere.monitor.jmx.ThreadPoolMXBean
- **Comments:** Available when the monitor-1.0 feature is enabled. See “Liberty:ThreadPool monitoring” on page 2269.

#### **8.5.5.0**

#### **WebSphere:feature=jaxws,type=WebServiceStats,service=\*,port=\***

- **Management interface:**org.apache.cxf.management.counters.ResponseTimeCounterMBean
- **Comments:** Available when the monitor-1.0 feature is enabled. The WebServiceStats can be either Performance.Counter.Server or Performance.Counter.client, where **service=\*** is the qualified name of a service endpoint, **port=\*** is the port name of the service endpoint. See “Liberty:JAX-WS monitoring” on page 2270.

**Note:** This is a Dynamic Model Mbean.

#### **8.5.5.0**

**8.5.5.0** WebSphere:feature=jaxws,type=Bus.Service.Endpoint,bus.id=\*,service=\*,port=\*,name=\*

- **Management interface:** org.apache.cxf.endpoint.ManagedEndpoint
- **Comments:** Available when the localConnector-1.0 or restConnector-1.0 feature is enabled and the JAX-WS application is accessed at least once. The **bus.id=\*** is the name of the bus, where \* is of the form <AppName>-Server-Bus. The **service=\*** is the qualified name of the endpoint, where \* is of the form {ServiceNamespace}ServiceName. The **port=\*** is the port name of the endpoint, where the \* is the

current port name. **8.5.5.0** The format of the MBean is as follows:

<BUS>@<SERVICE>@<PORT>@<URL\_PATTERN>, where:

- <BUS> is the same value as the field **bus.id**;
- <SERVICE> is the same value as the field **service**;
- <PORT> is the same value as the field **port**;
- <URL\_PATTERN> might be the following values in different scenarios;
  - If the url-pattern element is defined in the web.xml file of your application, the value of url-pattern element is used. For example, the url-pattern element is /SayHelloURL in the web.xml file:

```

<servlet-mapping>
  <servlet-name>com.ibm.ws.jaxws.test.jmx.service.WSTestEndpointService</servlet-name>
  <url-pattern>/SayHelloURL</url-pattern>
</servlet-mapping>

```

For example, the MBean might be as follows:

```

WebSphere:feature=jaxws,bus.id=EJBWSBasic-Server-Bus,type=Bus.Service.Endpoint,
service="{http://ejbbasic.jaxws.ws.ibm.com/}SayHelloService",port="SayHelloPort",
name="EJBWSBasic-Server-Bus@{http://ejbbasic.jaxws.ws.ibm.com/}SayHelloService@SayHelloPort@SayHelloURL"

```

- If the URL pattern is not specified, the service name is used as the default value. For example, the MBean might be as follows:

```

WebSphere:feature=jaxws,bus.id=EJBWSBasic-Server-Bus,type=Bus.Service.Endpoint,
service="{http://ejbbasic.jaxws.ws.ibm.com/}SayHelloService",port="SayHelloPort",
name="EJBWSBasic-Server-Bus@{http://ejbbasic.jaxws.ws.ibm.com/}SayHelloService@SayHelloPort@SayHelloService"

```

- If the URL pattern cannot be retrieved by the web services engine when the endpoint MBean is registered, a random unique number is used to ensure that the MBean is unique. For example, the MBean might be as follows:

```

WebSphere:feature=jaxws,bus.id=EJBWSBasic-Server-Bus,type=Bus.Service.Endpoint,
service="{http://ejbbasic.jaxws.ws.ibm.com/}SayHelloService",port="SayHelloPort",
name="EJBWSBasic-Server-Bus@{http://ejbbasic.jaxws.ws.ibm.com/}SayHelloService@SayHelloPort@261689241"

```

**Note:**

- This is a Dynamic Model Mbean.
- The destroy operation on this MBean is not supported.

**8.5.5.3**

**WebSphere:feature=kernel,name=ServerInfo**

- **Management interface:** com.ibm.websphere.kernel.server.ServerInfoMBean
- **Comments:** The ServerInfoMbean interface is used to retrieve information about the running server. Search the following directories for the class and API documentation:

```

liberty_home/dev/api/ibm/com.ibm.websphere.appserver.api.kernel.service_version-javadoc.zip
liberty_home/dev/api/ibm/com.ibm.websphere.appserver.api.kernel.service_version.jar

```

The exposed operations include a method to retrieve the product install and user directory locations, the default host name, the server name, the product version, the Java specification version, and the Java Runtime version.

**8.5.5.0**

**WebSphere:feature=wasJmsServer, type=MessagingEngine,name=\***

- **Management interface:** com.ibm.websphere.messaging.mbean.MessagingEngineMBean
- **Comments:** Available when the wasJmsServer-1.0 feature is enabled. One messaging engine instance is available for each Liberty. The **name=\*** is the name of the MBean, where \* is the unique name of the messaging engine MBean. See “Liberty:JMS messaging” on page 1010.

**8.5.5.0**

**WebSphere:feature=wasJmsServer, type=Queue,name=\***

- **Management interface:** com.ibm.websphere.messaging.mbean.QueueMBean
- **Comments:** The MBean is available when the wasJmsServer-1.0 feature is enabled and the MBean of the messaging engine is available. The **name=\*** is the name of the MBean, where \* is the name of the queue MBean. See “Liberty:JMS messaging” on page 1010.

**8.5.5.0**

**WebSphere:feature=wasJmsServer, type=Topic,name=\***

- **Management interface:**com.ibm.websphere.messaging.mbean.TopicMBean
- **Comments:** The MBean is available when the wasJmsServer-1.0 feature is enabled and the MBean of the messaging engine is available. The **name=\*** is the name of the MBean, where \* is the name of the topic MBean. See “Liberty:JMS messaging” on page 1010.

#### 8.5.5.0

**WebSphere:feature=wasJmsServer, type=Subscriber,name=\***

- **Management interface:**com.ibm.websphere.messaging.mbean.SubscriberMBean
- **Comments:** The MBean is available when the wasJmsServer-1.0 feature is enabled and the MBean of the messaging engine is available. The **name=\*** is the name of the MBean, where \* is the name of the subscriber MBean.

**Note:** The **SubscriberMBean** is a subscriber to the existing **TopicMBean**. See “Liberty:JMS messaging” on page 1010.

**Liberty:Examples of accessing MBean attributes and operations:** **8.5.0.1**

You can use Liberty to access the attributes, and call the operations, of Java Management Extensions (JMX) management beans (MBeans).

After you obtain an MBeanServer instance (for an application running on Liberty) or an MBeanServerConnection instance (for an external client), you can access the attributes or call the operations of MBeans provided by Liberty. See “Working with JMX MBeans on Liberty” on page 1646.

The following code examples assume the variable mbs is an MBeanServer or MBeanServerConnection instance. You can use the provided methods to access the attributes and operations in a similar way to Java reflection. Alternatively, each MBean has a management interface with getter methods for the attributes and methods for the operations. You can use these interfaces by implementing one of the javax.management.JMX.newMBeanProxy methods or one of the javax.management.JMX.newMXBeanProxy methods for MXBeans to obtain a proxy object. The name of a management interface ends with “MXBean”. For the names of the management interfaces, see “Liberty: List of provided MBeans” on page 1647.

#### Example 1: Check the state of application "myApp"

```
import javax.management.ObjectName;
import javax.management.JMX;
import com.ibm.websphere.application.ApplicationMBean;
...

ObjectName myAppMBean = new ObjectName(
    "WebSphere:service=com.ibm.websphere.application.ApplicationMBean,name=myApp");
if (mbs.isRegistered(myAppMBean)) {
    String state = (String) mbs.getAttribute(myAppMBean, "State");
    // alternatively, obtain a proxy object
    ApplicationMBean app = JMX.newMBeanProxy(mbs, myAppMBean, ApplicationMBean.class);
    state = app.getState();
}
```

#### Example 2: Get response time statistics for servlet "Example Servlet" from application "myApp"

```
import javax.management.ObjectName;
import javax.management.openmbean.CompositeData;
import javax.management.JMX;
import com.ibm.websphere.webcontainer.ServletStatsMXBean;
...


```

```

ObjectName servletMBean = new ObjectName("WebSphere:type=ServletStats,name=myApp.Example Servlet");
if (mbs.isRegistered(servletMBean)) {
    CompositeData responseTimeDetails = (CompositeData) mbs.getAttribute(servletMBean, "ResponseTimeDetails");
    CompositeData responseTimeReading = (CompositeData) responseTimeDetails.get("reading");
    Double mean = (Double) responseTimeReading.get("mean");
    Double standardDeviation = (Double) responseTimeReading.get("standardDeviation");
    // alternatively, obtain a proxy object
    ServletStatsMXBean servletStats = JMX.newMXBeanProxy(mbs, servletMBean, ServletStatsMXBean.class);
    StatisticsMeter meter = servletStats.getResponseTimeDetails();
    StatisticsReading reading = meter.getReading();
    mean = reading.getMean();
    standardDeviation = reading.getStandardDeviation();
}

```

### Example 3: Create a web server plug-in configuration file

```

import com.ibm.websphere.webcontainer.GeneratePluginConfigMBean;

...

ObjectName pluginMBean = new ObjectName("WebSphere:name=com.ibm.ws.jmx.mbeans.generatePluginConfig");
if (mbs.isRegistered(pluginMBean)) {
    mbs.invoke(pluginMBean, "generatePluginConfig", new Object[] {
        "installRoot", "serverName", new String[] {
            String.class.getName(), String.class.getName()
        }
    });
    // alternatively, use a proxy object
    GeneratePluginConfigMBean plugin = JMX.newMBeanProxy(mbs, name, GeneratePluginConfigMBean.class);
    plugin.generatePluginConfig("installRoot", "serverName");
}

```

#### 8.5.5.0

### Example 4: Query status of Web Service Endpoint

```

import javax.management.ObjectName;
import javax.management.MBeanServerConnection;
import javax.management.MBeanInfo;
import javax.management.MBeanAttributeInfo;
import javax.management.MBeanOperationInfo;

...

// Init mbs as needed
MBeanServerConnection mbs;

// Get MBeanInfo for specific ObjectName
ObjectName objName = new ObjectName("WebSphere:feature=jaxws,bus.id=testCXFJMXSupport-Server-Bus,
    type=Bus.Service.Endpoint,service=\"{http://jaxws.samples.ibm.com:jmx}/TestEndpointService\",
    port=\"TestEndpoint\",instance.id=1816106538");
MBeanInfo beanInfo = mbs.getMBeanInfo(objName);

// Go through attributes to find the interested one
for (MBeanAttributeInfo attr : beanInfo.getAttributes()) {
    if (attr.getName().equals("State")) {
        String status = String.valueOf(mbs.getAttribute(objName, attr.getName()));
        break;
    }
}

```

#### 8.5.5.0

### Example 5: Shut down the CXF server bus

```

import javax.management.ObjectName;
import javax.management.MBeanServerConnection;
import javax.management.MBeanInfo;
import javax.management.MBeanAttributeInfo;
import javax.management.MBeanOperationInfo;

...

// Init mbsc as needed
MBeanServerConnection mbs;

// Get MBeanInfo for specific ObjectName
ObjectName objName = new ObjectName("WebSphere:feature=jaxws,bus.id=testCXFJMXSupport-Server-Bus,
    type=Bus,instance.id=1618108530");

```

```

MBeanInfo beanInfo = mbsc.getMBeanInfo(objName);

// Go through operation to find the interested one and invoke
for (MBeanOperationInfo operation : beanInfo.getOperations()) {
    if (operation.getName().equals("shutdown")) {
        mbs.invoke(objName, operation.getName(), new Object[] { true }, new String[] { boolean.class.getName() });
        break;
    }
}

```

## Liberty:Examples of registering MBeans: **8.5.0.1**

An application can register its own MBean instances on Liberty. That MBean instance can then be used by other applications or external administrators.

Any application can register an MBean by using an MBeanServer instance. Suppose an application contains a class called `org.example.Example` that implements the interface `org.example.ExampleMBean`, which defines some attributes and operations. As in the following example, the application might simply instantiate the `Example` class then register it using a unique `ObjectName`. If the `ObjectName` chosen is already in use, a `javax.management.InstanceAlreadyExistsException` is reported.

```

import java.lang.management.ManagementFactory;
import javax.management.MBeanServer;
import javax.management.ObjectName;
import org.example.Example;

...

MBeanServer mbs = ManagementFactory.getPlatformMBeanServer();
Object mbean = new Example();
ObjectName name = new ObjectName("org.example.MyApplication:name=Example");
mbs.registerMBean(mbean, name);

```

In addition, an application might register an MBean that extends `java.lang.ClassLoader` and provides access to any number of MBean implementation classes. Then you can use any other JMX client, local or remote, to create and register MBeans provided by the application. For example, suppose the application has an MBean class `org.example.ApplicationClassLoader` that performs the following tasks:

- Implements any empty interface `org.example.ApplicationClassLoaderMBean`
- Extends `java.lang.ClassLoader`, and
- Provides access to the `org.example.Example` MBean implementation class

The application can register an instance of `ApplicationClassLoader` to make the `Example` MBean available to other JMX clients as follows:

```

import java.lang.management.ManagementFactory;
import javax.management.MBeanServer;
import javax.management.ObjectName;
import org.example.ApplicationClassLoader;

...

MBeanServer mbs = ManagementFactory.getPlatformMBeanServer();
Object classLoader = new ApplicationClassLoader();
ObjectName name = new ObjectName("org.example.MyApplication:name=ClassLoader");
mbs.registerMBean(classLoader, name);

```

Any JMX client can create an `Example` instance. The following example assumes the variable `mbs` is an `MBeanServer` or `MBeanServerConnection` instance. See “Working with JMX MBeans on Liberty” on page 1646.

```
import javax.management.ObjectName;

...

ObjectName loaderName = new ObjectName("org.example.MyApplication:name=ClassLoader");
ObjectName exampleName = new ObjectName("org.example.MyApplication:name=Example");
mbs.createMBean("org.example.Example", exampleName, loaderName);
```

If necessary, you can use other forms of the `MBeanServer.createMBean` method to create the MBean by using non-default constructors.

For more information about the management interface, see the Java API document for Liberty. The Java API documentation for each Liberty API is available in a separate .zip file in one of the javadoc subdirectories of the `{wlp.install.dir}/dev` directory.

### Liberty: Example of setting up a JMX routing environment: **8.5.5.0**

You can use Liberty to call Java Management Extensions (JMX) management beans (MBeans) on a collective member server through a collective controller server.

**Note:** **Distributed operating systems** **IBM i** The `collectiveController-1.0` feature and its capabilities are available only in WebSphere Application Server Liberty Network Deployment and WebSphere

Application Server Liberty for z/OS. **8.5.5.0** The feature is not available in WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core. If you have a WebSphere Application Server Liberty Network Deployment installation, you can use its `collectiveController-1.0` feature to work with collective members from WebSphere Application Server Liberty, WebSphere Application Server Liberty - Express, or WebSphere Application Server Liberty Core installations.

The `collectiveMember-1.0` feature enables a server to be managed by a collective controller (the `collectiveController-1.0` feature). After a server is configured to be managed by a collective controller, you can directly call any MBeans on the collective member through the collective controller server.

The following is an example of how to call MBeans on a collective member through a collective controller server.

```
// Set up the trust store to the collective controller server.

System.setProperty("javax.net.ssl.trustStore", "<trustStore for https connection to collective controller>");
System.setProperty("javax.net.ssl.trustStorePassword", "<trustStore password>");

Map<String, Object> environment = new HashMap<String, Object>();
environment.put("jmx.remote.protocol.provider.pkgs", "com.ibm.ws.jmx.connector.client");
environment.put(JMXConnector.CREDENTIALS, new String[] { "<username>", "<password>" });
environment.put(ClientProvider.DISABLE_HOSTNAME_VERIFICATION, true);
environment.put(ClientProvider.READ_TIMEOUT, 2 * 60 * 1000);

JMXServiceURL url = new JMXServiceURL(
    "REST", "<hostname of collective controller server>", "<https port>", "/IBMJMXConnectorREST");
jmxConnector = JMXConnectorFactory.connect(url, environment);
MBeanServerConnection exmbsc = jmxConnector.getMBeanServerConnection();

// You have a MBeanServerConnection now; at this point, however, all of your MBean calls
// are on the collective controller server.

// The next few lines of code are to set up the routing context so that all calls
// can be routed to a collective member.

ObjectName rmObjectName = new ObjectName(
    "WebSphere:feature=collectiveController,type=RoutingContext,name=RoutingContext");

// Call the MBeanRoutingContext MBean to set up the routing context.

Object rcObj = connection.invoke(rmObjectName, "assignServerContext",
    new Object[] {
```

```

    "<hostname of the collective member>", "<collective member server usr dir>", "<collective member server name>"
  },
// With the collective-member server usr dir and collective-member server name,
// the managed server can be uniquely identified on a host.

  new String[] { "java.lang.String", "java.lang.String", "java.lang.String" });

  if (rcObj instanceof Boolean) {
    Boolean result = (Boolean) rcObj;
    if (result.booleanValue()) {
      System.out.println("routing context is configured correctly");
    }
    Or if (!result.booleanValue()) {
      System.out.println("routing context result is false");
    }
  } else {
    System.out.println("failed to configure routing context");
  }
}

```

If the routing context is configured correctly, all future calls to this MBeanServerConnection will be routed to target collective member server.

## Establishing a JMX MBean Liberty server connection

8.5.5.0

You can use Jython-based scripts to establish a Java Management Extensions (JMX) MBean Liberty server connection.

### Before you begin

You must obtain and install the Jython version of your choice before you can perform this procedure. Without a Jython runtime, the instructions will fail.

### Procedure

1. Set up the environment.

The files that you need are located in *liberty\_home/clients/jython*.

- a. Copy the `lib/restConnector.py` file to *jython\_home/Lib*.
- b. Set the classpath for `restConnector.jar` in *liberty\_home/clients*.
 

```
set CLASSPATH=%CLASSPATH%;c:\wlp\clients\restConnector.jar
```

2. Run the utility.

**Example 1:** Getting a simple connection using `connector.connect(host,port,user,password)`

```

from restConnector import JMXRESTConnector
JMXRESTConnector.trustStore = "c:/key.jks"
JMXRESTConnector.trustStorePassword = "Liberty"

```

```

connector = JMXRESTConnector()
connector.connect("foo.bar.com",9443,"theUser","thePassword")
mconnection = connector.getMBeanServerConnection()
# mconnection.invoke(...)
connector.disconnect()

```

**Example 2:** Getting an advanced connection using `connector.connect(host,port,map)` with user-provided properties

```

import java
import javax
import jarray
import com.ibm.websphere.jmx.connector.rest
import com.ibm.ws.jmx.connector.client.rest

map=java.util.HashMap()
map.put("jmx.remote.provider.pkgs","com.ibm.ws.jmx.connector.client")
map.put(javax.management.remote.JMXConnector.CREDENTIALS,jarray.array(["theUser","thePassword"],java.lang.String))

```

```

map.put(com.ibm.ws.jmx.connector.client.rest.ClientProvider.READ_TIMEOUT,2*60*1000)
map.put(com.ibm.websphere.jmx.connector.rest.ConnectorSettings.DISABLE_HOSTNAME_VERIFICATION, True)

connector = JMXRESTConnector()
connector.connect("foo.bar.com",9443,map)
mconnection = connector.getMBeanServerConnection()
# mconnection.invoke(...)
connector.disconnect()

```

### Example 3: Registering a notification listener

```

import java
import javax

from restConnector import JMXRESTConnector
from restConnector import BaseNotificationListener

class SampleNotificationListener(BaseNotificationListener):
    def __init__(self):
        pass

    def handleNotification(self,notification,handback):
        print "Notification received:"
        print " Source: " + notification.getSource().toString()
        print " Type: " + notification.getType()
        print " Message: " + notification.getMessage()

# main starts here

JMXRESTConnector.trustStore = "c:/key.jks"
JMXRESTConnector.trustStorePassword = "Liberty"

connector=JMXRESTConnector()
connector.connect("foo.bar.com",9443,"theUser","thePassword")
mconnection=connector.getMBeanServerConnection()

listener=SampleNotificationListener()
handback=java.lang.Object()

notifier1=javax.management.ObjectName("web:name=Notifier1")
mconnection.addNotificationListener(notifier1,listener,None,handback)

```

#### **JMXRESTConnector.trustStore**

Sets the path to where the SSL key file is stored

#### **JMXRESTConnector.trustStorePassword**

Sets the password for the key

#### **JMXRESTConnector.connect(host,port,user,password)**

Creates a connector to the server

#### **JMXRESTConnector.connect(host,port,map)**

Creates a connector with user properties

#### **JMXRESTConnector.getMBeanServerConnection**

Gets a connection to the MBean server

#### **JMXRESTConnector.disconnect()**

Closes the connection

## What to do next

After a connection to the MBean server is established, you can make calls to the MBean server by using the `invoke(...)` method.

**Note:** A library of Jython scripts is available for you to download from the Liberty Repository.

## Liberty: File transfer

The restConnector-1.0 feature includes the FileTransfer and FileService MBeans. The FileTransfer MBean supports delete, upload, and download operations to and from a running Liberty server. The FileService MBean provides access to directory lists and file metadata, and it also provides archive operations such as **create** and **expand**.

The FileTransfer and FileService MBeans are useful for carrying out remote operations on a Liberty, such as updating the configuration or installing an application. A configuration update can be performed remotely by uploading an updated server.xml file for the target Liberty server. An application can be installed by uploading both the application archive and an updated server.xml file or simply by uploading the application archive to the monitored dropins folder.

The FileTransfer MBean includes configurable read and write lists so that you can control the directories that can be read or written when using the FileTransfer MBean.

**8.5.0.1** See the section on the FileTransfer MBean in “Liberty: List of provided MBeans” on page 1647 for information on how to configure the restConnector-1.0 feature and control the FileTransfer MBean read and write lists.

The uploadFile method from FileTransfer contains a boolean called "expandOnCompletion" that allows a user to upload and expand the archive with a single MBean invocation. A directory is created with the same name as the archive on the target path and the FileService MBean is automatically invoked to expand the archive.

**Example:** A call to uploadFile with parameters {"C:/temp/myArchive.zip", "\${server.output.dir}/myArchive.zip", true} will result in a myArchive.zip directory under \${server.output.dir} that contains the extracted contents of the archive being created.

## Transferring files in a Liberty collective

### 8.5.5.0

A Liberty controller enables special file transfer capabilities within a Liberty collective. The most advanced such functionality is file transfer for multiple hosts within a single REST call. You can use the FileTransfer and FileService MBeans in a Liberty collective to perform file actions on any Liberty server in the collective. This includes both Liberty servers configured as collective controllers and as collective members.

### About this task

When you establish a remote JMX connection to a collective controller, you can use the RoutingContext MBean to direct your FileTransfer and FileService MBean calls to execute on any Liberty server in the collective. The collective controller takes care of routing the request and creating authorized connections between the collective controller and the target collective member.

By routing file operations to specific collective members, you can perform configuration-file updates and install applications on any Liberty server in the collective.

The FileTransfer MBean additionally can perform operations on a host computer in a collective whether or not there is a collective member on that host. By registering the host computer with the Liberty collective and specifying a RoutingContext that specifies that host, the FileTransfer command can be used to upload or download files to or from that host system. For example, you can upload and expand a Liberty archive to push out Liberty to new hosts.

The upload and extract operation in a routing environment has a more complex logic than that in the non-routing environment:

- If the target host machine has access to an **unzip** command on its path, that command is invoked to extract the archive.
- If an **unzip** command is not found, the process uses a Java-based archive extraction.
  1. A small Liberty-built jar file is temporarily pushed into the target host.
  2. A path to Java is found by checking the following:
    - Configured Java-home value that was setup during host registration
    - Configured JAVA\_HOME variable visible to RXA
    - Configured JRE\_HOME variable visible to RXA
    - Java home found on the path
  3. The custom Java jar file is invoked to extract the original archive.
  4. The custom Java jar file is deleted from the target host.
  5. If the archive being expanded by the custom Java jar file is a Liberty archive, the process recursively sets the permissions of its wlp/bin folder to 755 to allow for remote management of that Liberty instance.

The FileTransfer MBean uses authorization information stored in the collective controller for either the target host computer or collective member. This information was stored when the host computer or collective member was registered. See “Registering host computers with a Liberty collective” on page 1142 for more information on setting up this information for the host computer.

File-transfer operations directed at the host computer use the authorization information stored for the host computer. File-transfer operations directed at a collective member use the authorization overridden by the collective member, if any, or use the information stored for the host computer by default. See “Overriding Liberty server host information” on page 1144 for more information on overriding host information.

The FileService MBean operates on Liberty (not only on host computers) and uses the authorization configurations from Liberty. It does not use host-computer authorization information.

## Transferring files to and from a collective member or registered host with REST calls

8.5.5.6

You can perform routed file transfer operations from a collective controller to a collective member or to a registered host of a collective by invoking REST APIs. The operations include downloading files from a remote location, uploading files to a remote location, and deleting files in a remote location. Use the **GET**, **POST**, or **DELETE** REST APIs. The file transfer operations occur within an IBM JMX REST Connector.

### Before you begin

To perform file transfer operations from a collective controller to a member server, the server must be joined as a member to the collective. See “Configuring a Liberty collective” on page 1136.

To perform file transfer operations to a host computer, the host must be registered with the collective controller. See “Registering host computers with a Liberty collective” on page 1142.

### Procedure

1. Optional: To read about the REST APIs, point a browser at `https://controller_host_name:controller_port_name/IBMJMXConnectorREST/api` and enter the controller administrative user ID and password to log in. The controller must be running to view the REST API documentation. Alternatively, you can use a collective member host, port, login user ID and password to view the REST API documentation.

The **File Transfer** and **Routing** sections describe the APIs used to transfer files between the collective controller and a member server or a registered host.

The `collectiveController-1.0` and `collectiveMember-1.0` features enable the `restConnector-1.0` feature, which provides file transfer capability. Thus, collective controllers and members do not need to specify `restConnector-1.0` in a feature manager to view the REST APIs or perform file transfer operations. A stand-alone server configuration might need the `restConnector-1.0` feature to view the REST APIs.

2. Unless you work directly with a Liberty instance, set the routing context as HTTP headers.

- Member server routing

```
com.ibm.websphere.jmx.connector.rest.routing.hostName=string
com.ibm.websphere.jmx.connector.rest.routing.serverName=string
com.ibm.websphere.jmx.connector.rest.routing.serverUserDir=string
```

- Registered host routing

```
com.ibm.websphere.jmx.connector.rest.routing.hostName=string
```

3. Ensure the target file is within the configurable read/write directories of the server for file transfer operations with a member server, or within configurable read/write directories of the host for file transfer operations with a registered host.

4. Invoke REST APIs that download, upload, or delete files.

`{filePath}` must be URL-encoded. For routing operations with registered hosts, `{filePath}` must be an absolute path and cannot contain Liberty variables.

- Download one file from a member server or registered host using the **GET** operation.

```
GET https://controller_host:controller_port/IBMJMXConnectorREST/file/{filePath}
```

- Upload one file to a member server or registered host using the **POST** operation.

```
POST https://controller_host:controller_port/IBMJMXConnectorREST/file/{filePath}
```

- Delete one file from a member server or registered host using the **DELETE** operation.

```
DELETE https://controller_host:controller_port/IBMJMXConnectorREST/file/{filePath}
```

- Delete multiple files from a member server or registered host using the **POST** operation.

```
POST https://controller_host:controller_port/IBMJMXConnectorREST/file/collection
```

## Example

To download the `myFile.txt` file from the member server `myServerA` on the host `myTarget.com` with a user directory of `C:/server/wlp`:

1. Set the member server routing context as HTTP headers.

```
com.ibm.websphere.jmx.connector.rest.routing.hostName=myTarget.com
com.ibm.websphere.jmx.connector.rest.routing.serverName=myServerA
com.ibm.websphere.jmx.connector.rest.routing.serverUserDir=C:/server/wlp
```

2. Invoke a **GET** call to download the file.

```
GET https://myTarget.com:9443//IBMJMXConnectorREST/file/C%3A%2Ftemp%2FmyFile.txt
```

To download the `myFile.txt` file from the registered host `myTarget.com`:

1. Set the registered host routing context as an HTTP header.

```
com.ibm.websphere.jmx.connector.rest.routing.hostName=myTarget.com
```

2. Invoke a **GET** call to download the file.

```
GET https://myTarget.com:9443//IBMJMXConnectorREST/file/C%3A%2Ftemp%2FmyFile.txt
```

To download the `server.xml` file from the member server `myServerA` on the host `myTarget.com` with a user directory of `C:/server/wlp`:

1. Set the member server routing context as HTTP headers.

```
com.ibm.websphere.jmx.connector.rest.routing.hostName=myTarget.com
com.ibm.websphere.jmx.connector.rest.routing.serverName=myServerA
com.ibm.websphere.jmx.connector.rest.routing.serverUserDir=C:/server/wlp
```

2. Invoke a **GET** call to download the `${server.config.dir}/server.xml` file.

```
GET https://myTarget.com:9443//IBMJMXConnectorREST/file/%24{server.config.dir}%2Fserver.xml
```

## What to do next

Get status or details on the REST call. See “Getting status on a REST call for multiple registered hosts” on page 1665.

## Uploading files to multiple registered hosts with a single REST call

8.5.5.6

You can upload files from a collective controller to multiple registered hosts of a collective by invoking the **POST** REST API. The file transfer operations occur within an IBM JMX REST Connector.

### Before you begin

Create a collective controller. See “Configuring a Liberty collective” on page 1136.

Register each remote host computer with the collective controller. See “Registering host computers with a Liberty collective” on page 1142.

### Procedure

1. Optional: To read about the REST APIs, point a browser at `https://controller_host_name:controller_port_name/IBMJMXConnectorREST/api` and enter the controller administrative user ID and password to log in. The controller must be running to view the REST API documentation.

The **File Transfer** and **Routing** sections describe the APIs used to transfer files between the collective controller and a member server or a registered host.

The `collectiveController-1.0` feature enables the `restConnector-1.0` feature, which provides file transfer capability. Thus, collective controllers do not need to specify `restConnector-1.0` in a feature manager to view the REST APIs or perform file transfer operations. A stand-alone server configuration might need the `restConnector-1.0` feature to view the REST APIs.

2. List the target hosts in an HTTP header for the collective controller.

```
com.ibm.websphere.collective.hostNames=comma-separated_list_of_target_hosts
```

Optionally, set other HTTP headers:

- Specify whether to perform the file uploads and the action asynchronously. Default is `false`. To change the default, specify `true` for *boolean*.

```
com.ibm.websphere.jmx.connector.rest.asyncExecution=boolean
```

- Specify a set of actions to perform after the file uploads. An existing built-in action is `com.ibm.websphere.jmx.connector.rest.postTransferAction.join`, which joins the Liberty servers inside the incoming Liberty archive to the collective. Use the header to list other custom actions. If you list more than one custom action, delimit the action with a URL-encoded comma character.

```
com.ibm.websphere.jmx.connector.rest.postTransferAction=comma-separated_list_of_actions
```

To enable the custom actions, add the following configuration to the collective controller `server.xml`:

```
<hostAccess enableCustomActions="true" />
```

- Specify a list of options to pass into the post-transfer actions. This list of options must be either null or contain the same number of list items as the `postTransferAction` header list, where the item index of each option must match the index of its corresponding action. If you list more than one option, delimit the action with a URL-encoded comma character.

```
com.ibm.websphere.jmx.connector.rest.postTransferAction.options=comma-separated_list_of_options
```

If you specify the built-in action `com.ibm.websphere.jmx.connector.rest.postTransferAction.join`, the corresponding option must be:

```
--user=adminUser --password=adminPw --keystorePassword=keystorePw [--rpcUser=rpcUser --rpcPassword=rpcPw]
```

- Specify environment variables to set before the transfer actions run. The payload of the header is a JSON object where each JSON key is an environment variable and each JSON value is its corresponding value. If you specify system paths, use forward slashes (/).

```
com.ibm.websphere.jmx.connector.rest.transferEnvVars=list_of_environment_variables
```

### 3. Upload a file to multiple registered hosts by using the **POST** operation.

- a. Ensure that the target location is within a configurable write directory of the hosts.
- b. Invoke the **POST** operation.

```
POST https://controller_host:controller_port/IBMJMXConnectorREST/file/{filePath}[?expandOnCompletion=boolean&local=boolean]
```

- `{filePath}` is a UTF-8 URL-encoded absolute path that specifies the target location. For example, if the file is `C:/temp/myFile.txt`, the path is `C%3A%2Ftemp%2FmyFile.txt`.
- `expandOnCompletion` is an optional query parameter that toggles an automatic expansion of the uploaded archive. The default value is `false`.
- `local` is an optional query parameter that specifies whether the file to upload is already in the controller. If true, then the payload of this **POST** request is a string that represents the source file location inside the controller. The default value is `false`.
- If the `local` query parameter is not used, or explicitly set to `false`, the **POST** payload is the binary content of the source file itself.

## What to do next

Get status or details on the REST call. See “Getting status on a REST call for multiple registered hosts” on page 1665.

## Deleting files from multiple registered hosts with a single REST call

8.5.5.6

You can delete files on multiple registered hosts of a collective from a collective controller by invoking the **DELETE** REST API. The file deletions occur within an IBM JMX REST Connector.

### Before you begin

Create a collective controller. See “Configuring a Liberty collective” on page 1136.

Register each remote host computer with the collective controller. See “Registering host computers with a Liberty collective” on page 1142.

### Procedure

1. Optional: To read about the REST APIs, point a browser at `https://controller_host_name:controller_port_name/IBMJMXConnectorREST/api` and enter the controller administrative user ID and password to log in. The controller must be running to view the REST API documentation.

The **File Transfer** and **Routing** sections describe the APIs used to transfer files between the collective controller and a member server or a registered host.

The `collectiveController-1.0` feature enables the `restConnector-1.0` feature, which provides file transfer capability. Thus, collective controllers do not need to specify `restConnector-1.0` in a feature manager to view the REST APIs or perform file transfer operations. A stand-alone server configuration might need the `restConnector-1.0` feature to view the REST APIs.

2. List the target hosts in an HTTP header for the collective controller.

```
com.ibm.websphere.collective.hostNames=comma-separated_list_of_target_hosts
```

Optionally, set other HTTP headers:

- Specify whether to perform the file deletion and the action asynchronously. Default is `false`. To change the default, specify `true` for `boolean`.

```
com.ibm.websphere.jmx.connector.rest.asyncExecution=boolean
```

- Specify a set of actions to perform before the file deletion. An existing built-in action is `com.ibm.websphere.jmx.connector.rest.preTransferAction.remove`, which removes the Liberty servers inside the Liberty directory to be deleted from the collection. Use the header to list other custom actions. If you list more than one custom action, delimit the action with a URL-encoded comma character.

```
com.ibm.websphere.jmx.connector.rest.preTransferAction=comma-separated_list_of_actions
```

To enable the custom actions, add the following configuration to the collective controller `server.xml`:

```
<hostAccess enableCustomActions="true" />
```

- Specify a list of options to pass into the pre-transfer actions. This list of options must be either null or contain the same number of list items as the `preTransferAction` header list, where the item index of each option must match the index of its corresponding action. If you list more than one option, delimit the action with a URL-encoded comma character.

```
com.ibm.websphere.jmx.connector.rest.preTransferAction.options=comma-separated_list_of_options
```

If you specify the built-in action

`com.ibm.websphere.jmx.connector.rest.preTransferAction.remove`, the corresponding option must be:

```
--user=adminUser --password=adminPw --keystorePassword=keystorePw [--rpcUser=rpcUser --rpcPassword=rpcPw]
```

- Specify credentials to use for the delete action. The payload of the header is a JSON object where each JSON key is an environment variable and each JSON value is its corresponding value. If you specify system paths, use forward slashes (/).

```
com.ibm.websphere.jmx.connector.rest.transferCredentials=list_of_environment_variables
```

- Specify environment variables to set before the actions run. The payload of the header is a JSON object where each JSON key is an environment variable and each JSON value is its corresponding value. If you specify system paths, use forward slashes (/).

```
com.ibm.websphere.jmx.connector.rest.transferEnvVars=list_of_environment_variables
```

### 3. Delete a file from multiple registered hosts using the **DELETE** operation.

- a. Ensure the target location is within a configurable write directory of the hosts.
- b. Invoke the **DELETE** operation.

```
DELETE https://controller_host:controller_port/IBMJMXConnectorREST/file/{filePath}[?recursiveDelete=boolean]
```

- `{filePath}` is a UTF-8 URL-encoded absolute path that specifies the target location. For example, if the file is `C:/temp/myFile.txt`, the path is `C%3A%2Ftemp%2FmyFile.txt`.
- `recursiveDelete` is an optional query parameter that deletes non-empty directories. The default value is `false`.

## What to do next

Get status or details on the REST call. See “Getting status on a REST call for multiple registered hosts.”

## Getting status on a REST call for multiple registered hosts

8.5.5.6

You can get status or details about a call to upload or delete files on multiple registered hosts of a collective by invoking the **GET REST** API.

## Before you begin

Call a REST API to upload or delete files on multiple registered hosts. See “Uploading files to multiple registered hosts with a single REST call” on page 1663 or “Deleting files from multiple registered hosts with a single REST call” on page 1664.

## Procedure

- Get overall multiple task status, with the option of filtering the results.

```
GET https://controller_host:controller_port/IBMJMXConnectorREST/file/status/[?key=value]
```

The *key* variable is a task property filtered with the *value* variable. You can specify multiple *key=value* pairs to use as query filters.

- Get status about a specific task.

```
GET https://controller_host:controller_port/IBMJMXConnectorREST/file/status/{taskID}
```

*{taskID}* represents a task; for example, c8a2b96b-5a6a-493c-ad0c-140df87d61cf.

- Get a list of available properties from a specific task.

```
GET https://controller_host:controller_port/IBMJMXConnectorREST/file/status/{taskID}/properties
```

*{taskID}* represents a task; for example, c8a2b96b-5a6a-493c-ad0c-140df87d61cf.

- Get the value of a property in a specific task.

```
GET https://controller_host:controller_port/IBMJMXConnectorREST/file/status/{taskID}/properties/{property}
```

– *{taskID}* represents a task; for example, c8a2b96b-5a6a-493c-ad0c-140df87d61cf.

– *{property}* represents the property to get.

- Get status about the hosts of a specific task.

```
GET https://controller_host:controller_port/IBMJMXConnectorREST/file/status/{taskID}/hosts
```

*{taskID}* represents a task; for example, c8a2b96b-5a6a-493c-ad0c-140df87d61cf.

- Get details about steps that were taken within a specific host of a specific task.

```
GET https://controller_host:controller_port/IBMJMXConnectorREST/file/status/{taskID}/hosts/{hostName}
```

– *{taskID}* represents a task; for example, c8a2b96b-5a6a-493c-ad0c-140df87d61cf.

– *{hostName}* represents a host; for example, machineA.xyz.com.

## Example

Get overall multiple task status, with the option of filtering the results. If the JSON response is:

```
[
  {
    "taskID" : String ,
    "taskStatus" : String,
    "taskURL" : URL
  }*
]
```

For the following **GET** call:

```
GET https://myTarget.com:9443/IBMJMXConnectorREST/file/status
```

Typical status is:

```
[
  {
    "taskID" : "c8a2b96b-5a6a-493c-ad0c-140df87d61cf" ,
    "taskStatus" : "succeeded",
    "taskURL" : "/IBMJMXConnectorREST/file/status/c8a2b96b-5a6a-493c-ad0c-140df87d61cf"
  },
  {
    "taskID" : "18c807ff-e7bb-4584-a988-278039d0aabd" ,
    "taskStatus" : "failed",
    "taskURL" : "/IBMJMXConnectorREST/file/status/18c807ff-e7bb-4584-a988-278039d0aabd"
  }
]
```

For the following **GET** call with two *key=value* pairs:

```
GET https://myTarget.com:9443/IBMJMXConnectorREST/file/status?user=bob&status=succeeded
```

Typical status is:

```
[
  {
    "taskId" : "c8a2b96b-5a6a-493c-ad0c-140df87d61cf" ,
    "taskStatus" : "succeeded",
    "taskURL" : "/IBMJMXConnectorREST/file/status/c8a2b96b-5a6a-493c-ad0c-140df87d61cf"
  }
]
```

## Configuring binary logging in Liberty

**8.5.5.0**

Use this information as a guide for configuring binary logging in your Liberty.

### About this task

Binary logging provides faster log and trace handling capabilities and more flexible ways to use log and trace content than the default Liberty log and trace framework.

A server configuration consists of a `bootstrap.properties` file, a `server.xml` file, and any (optional) files that are included with those files. The `bootstrap.properties` file specifies properties that need to be available before the main configuration is processed, and are kept to a minimum. The `server.xml` file is the primary configuration file for the server.

The `server.xml` file and its associated files use a simple xml format that is suitable for most text editors.

**Distributed operating systems** A richer editing experience is provided by the eclipse server adapter for Liberty (WAS4D+ adapter), which uses a generated schema to provide drop-down lists of available choices, auto-completion, and other editing tools. For a description of the eclipse server adapter for Liberty, see “Editing the Liberty configuration by using developer tools” on page 1556.

The `bootstrap.properties` file specifies whether the server uses binary logging as the log and trace framework, or the default log and trace framework. A server restart is required to switch between binary logging and the default log and trace framework.

You can modify the configuration of binary logging through the server configuration or the `bootstrap.properties` file.

- **Server configuration:** To get logging from your own code, which is loaded after server configuration processing, use the server configuration to configure binary logging.
- **bootstrap.properties file:** You might need to set logging properties to take effect before the server configuration files are processed. For example, if you need to analyze problems that occur early in server start or configuration processing. In this case, you can configure binary logging in the `bootstrap.properties` file.

You can set Logging properties in either the `bootstrap.properties` or the `server.xml` file. Use attributes in the `server.xml` file, or use equivalent properties in the `bootstrap.properties` file. Any settings in the `bootstrap.properties` file are used from the time the server reads the `bootstrap.properties` file until the time the `server.xml` file is processed. If the logging properties in the `bootstrap.properties` file are not replaced or reset in the `server.xml` file, the property values in the `bootstrap.properties` file continue to be used.

When binary logging is enabled, the `maxFileSize`, `maxFiles`, `messageFileName`, `traceFileName`, and `traceFormat` logging element attributes are ignored (since binary logging runs without `trace.log` and `messages.log` files). The `traceSpecification`, `consoleLogLevel`, and `logDirectory` attributes continue to be used to set the trace specification, the level for the console log, and the placement of the log and trace files.

If you set logging or binary logging attributes in the `server.xml` file, you can avoid changes in configuration between startup time and runtime by setting the corresponding properties in the `bootstrap.properties` file to the same value. If no logging or binary logging properties are set in the `bootstrap.properties` file, the server uses the default logging settings.

## Procedure

- Enable binary logging for the server by updating the `bootstrap.properties` file. In the `bootstrap.properties` file, add the following text on a line by itself:  
`websphere.log.provider=binaryLogging-1.0`
- Use the following parameters to configure binary logging. All subelements that are listed are subelements of the logging element in the `server.xml` file. The following table lists the attributes that are configurable in the `server.xml` file and the equivalent properties that can be set in the `bootstrap.properties` file:

*Table 119. Binary logging attributes that are configurable in `server.xml` and the equivalent properties that can be set in `bootstrap.properties`*

Logging subelement	Attribute	Equivalent <code>bootstrap.properties</code> property
binaryLog	purgeMaxSize	<code>com.ibm.hpel.log.purgeMaxSize</code>
	purgeMinTime	<code>com.ibm.hpel.log.purgeMinTime</code>
	fileSwitchTime	<code>com.ibm.hpel.log.fileSwitchTime</code>
	bufferingEnabled	<code>com.ibm.hpel.log.bufferingEnabled</code>
	outOfSpaceAction	<code>com.ibm.hpel.log.outOfSpaceAction</code>
binaryTrace	purgeMaxSize	<code>com.ibm.hpel.trace.purgeMaxSize</code>
	purgeMinTime	<code>com.ibm.hpel.trace.purgeMinTime</code>
	fileSwitchTime	<code>com.ibm.hpel.trace.fileSwitchTime</code>
	bufferingEnabled	<code>com.ibm.hpel.trace.bufferingEnabled</code>
	outOfSpaceAction	<code>com.ibm.hpel.trace.outOfSpaceAction</code>

The following example shows a `bootstrap.properties` file that is configured to enable binary logging:

```
websphere.log.provider=binaryLogging-1.0
```

The following example shows a `server.xml` file with the binary logging subelements. The log content is set to expire after 96 hours and the trace content is set to retain a maximum of 1024MB:

```
<server description="new server">
  <logging>
    <binaryLog purgeMinTime="96"/>
    <binaryTrace purgeMaxSize="1024"/>
  </logging>
</server>
```

For the full logging configuration reference, see the logging, binaryLog, and binaryTrace elements in the .

## Results

After you restart the server, binary logging is enabled and configured.

## Administering the transaction service on Liberty

**8.5.5.0**

Liberty provides many of the same transaction services that are provided in the WebSphere Application Server traditional. If an application uses two or more resources, the Liberty transaction manager coordinates the updates to all the resource managers under the control of a global transaction. In Liberty, transaction services are implicitly activated when you specify features that require the use of transactions; for example, jpa-2.0, jdbc-4.0, and wasJmsServer-1.0.

## About this task

You can control when database transaction recovery occurs, you can specify configuration settings that determine how database transactions are recovered, and you can choose whether to store your transaction logs as operating system files or in a relational database.

## Liberty: Configuring the startup of the transaction service

8.5.5.0

Database transaction recovery can occur either when the transaction service is first used, or at server startup.

## About this task

By default, transaction recovery after a server failure happens when the transaction service is first used rather than at server startup. You can alter this behavior by specifying transaction service attributes that control when recovery happens, and whether the system waits for recovery to finish before allowing transactional work to proceed.

## Procedure

To configure transaction service startup, specify the following attributes in the transaction element in the server.xml file:

- recoverOnStartup

This attribute can take the following values:

- true: Transaction recovery occurs at server startup.
- false: Transaction recovery occurs when the transaction service is first used.

- waitForRecovery

This attribute can take the following values:

- true: The server waits for transaction recovery to finish before allowing transactional work to proceed.
- false: The server allows transactional work to proceed without waiting for transaction recovery to finish.

## Example

With the following transaction element configuration, transaction recovery occurs at server startup, and the server waits for transaction recovery to finish before allowing transactional work to proceed.

```
<transaction
  recoverOnStartup="true"
  waitForRecovery="true"
/>
```

## Liberty:How database transactions are recovered

When the Liberty transaction manager recovers indoubt database transactions, it uses either the unique identifier or the JNDI name to locate the current dataSource element, and then determines the user ID and password to use for recovery.

Configure a data source by specifying the attributes of the `dataSource` element in the `server.xml` configuration file. You can assign a unique identifier or a **jndiName** attribute for the data source as follows:

```
<dataSource id="ds1" jndiName="jdbc/ds1"... />
```

You must not change the value of the **id** or **jndiName** attribute when a recovery is pending for a transaction in which the data source participated. If you change any other attributes of the `dataSource` element, those changes are retained for the recovery. Therefore, you can, for example, add a **recoveryAuthDataRef** attribute that specifies a database user ID and password to use for recovery.

The database user ID and password to use for recovery are determined according to the following order of precedence:

1. If the `dataSource` element has the **recoveryAuthDataRef** attribute defined, then the user ID and password from the `authData` element are used. For example:

```
<authData id="recoveryAuth" user="dbuser1" password="{xor}0z0vKDtu"/>
<dataSource id="ds1" jndiName="jdbc/ds1" jdbcDriverRef="DB2"
  recoveryAuthDataRef="recoveryAuth" .../>
```

2. If container-managed authentication is used, then the user ID and password from the container-managed authentication alias are used. For example:

- In the `ibm-web-bnd.xml` file, you have the following code:

```
<resource-ref name="jdbc/ds1ref" binding-name="jdbc/ds1">
  <authentication-alias name="user1Auth"/>
</resource-ref>
```

- In the `server.xml` file, you must define the following code:

```
<authData id="user1Auth" user="dbuser1" password="{xor}0z0vKDtu"/>
<dataSource id="ds1" jndiName="jdbc/ds1" jdbcDriverRef="DB2" .../>
```

3. The user ID and password from the `dataSource` element are used. For example:

```
<dataSource id="ds1" jndiName="jdbc/ds1" jdbcDriverRef="DB2" ...>
  <properties.db2.jcc databaseName="testdb" user="dbuser1" password="{xor}0z0vKDtu"/>
</dataSource>
```

4. If none of the previous conditions are satisfied, and the recovery is attempted without any user ID and password, then the behavior is determined by the JDBC driver and database.

**Note:** If the transaction recovery is performed by an application-defined data source, such as an `@DataSourceDefinition` annotation or a `<data-source>` element in the deployment descriptor, you must ensure that the associated application is running when the recovery is taking place. You cannot use configuration settings in the `server.xml` file to recover application-defined data sources.

## Liberty: Storing transaction logs in a relational database

### 8.5.5.0

You can choose to store your Liberty transaction logs in a relational database rather than as operating system files. In WebSphere Application Server traditional, this feature provides high availability (HA) support without having to use a shared file system. The feature is provided in Liberty for compatibility and for evaluation and testing purposes.

### About this task

The WebSphere Application Server transaction service writes information to a transaction log for every global transaction that involves two or more resources, or that is distributed across multiple servers. These transactions are started or stopped either by applications or by the container in which they are deployed. The transaction service maintains transaction logs to ensure the integrity of transactions. Information is written to the transaction logs in the prepare phase of a distributed transaction, so that if a

WebSphere Application Server with active transactions restarts after a failure, the transaction service is able to use the logs to replay any indoubt transactions. This allows the overall system to be brought back to a consistent state.

In previous releases of WebSphere Application Server, the transaction logs were stored as operating system files. In WebSphere Application Server Version 8.5.5 and later, this remains the default configuration but you can choose to store the transaction logs in a relational database management system (RDBMS). This configuration option is aimed at customers working in an HA environment. In previous releases of WebSphere Application Server, HA transaction support required the use of a shared file system to host the transaction logs, such as an NFSv4-mounted network attached storage (NAS) or a storage area network (SAN). This new feature allows customers, particularly those with an investment in HA database technology, to use their HA database as a shared repository for the transaction logs, as an alternative to using a shared file system.

By default, Liberty transaction logs are stored in operating system files. However, for compatibility with WebSphere Application Server traditional, and for evaluation and testing purposes, you can configure the transaction logs to be stored in an RDBMS. You can use any database type that is supported by Liberty.

## Procedure

To configure the Liberty transaction logs to be stored in an RDBMS, complete the following steps:

1. Configure a dedicated, non-transactional data source in the Liberty `server.xml` file.

The following example extract from the `server.xml` file shows how to configure Liberty to store its transaction logs in a DB2 database:

```
<transaction>
  <dataSource transactional="false">
    <jdbcDriver libraryRef="DB2JCC4LIB"/>
    <properties.db2.jcc currentSchema="CBIVP"
      databaseName="SAMPLE" driverType="4"
      portNumber="50000" serverName="localhost"
      user="db2admin" password="{xor}0z1tPjsyNjE=" />
    </dataSource>
  </transaction>

<library id="DB2JCC4LIB">
  <fileset dir="C:/SQLLIB/java" includes="db2jcc4.jar db2jcc_license_cu.jar"/>
</library>
```

2. (optional) Create the database tables.

Liberty attempts to create the necessary database tables when the server first starts. When this is not possible, due to insufficient permission for example, the server fails to start. Under these circumstances, you must create the two required database tables manually.

The following DDL structures show how to create the tables on DB2:

```
CREATE TABLE WAS_TRAN_LOG(
  SERVER_NAME VARCHAR(128),
  SERVICE_ID SMALLINT,
  RU_ID BIGINT,
  RUSECTION_ID BIGINT,
  RUSECTION_DATA_INDEX SMALLINT,
  DATA LONG VARCHAR FOR BIT DATA)

CREATE TABLE WAS_PARTNER_LOG(
  SERVER_NAME VARCHAR(128),
  SERVICE_ID SMALLINT,
  RU_ID BIGINT,
  RUSECTION_ID BIGINT,
  RUSECTION_DATA_INDEX SMALLINT,
  DATA LONG VARCHAR FOR BIT DATA)
```

The following DDL structures shows how to create the database table on Oracle:

```

CREATE TABLE WAS_TRAN_LOG(
  SERVER_NAME VARCHAR(128),
  SERVICE_ID SMALLINT,
  RU_ID NUMBER(19),
  RUSECTION_ID NUMBER(19),
  RUSECTION_DATA_INDEX SMALLINT,
  DATA BLOB)

CREATE TABLE WAS_PARTNER_LOG(
  SERVER_NAME VARCHAR(128),
  SERVICE_ID SMALLINT,
  RU_ID NUMBER(19),
  RUSECTION_ID NUMBER(19),
  RUSECTION_DATA_INDEX SMALLINT,
  DATA BLOB)

```

## Administering data access resources on Liberty

Administer data access resources using the Liberty features for JDBC, MongoDB, and more.

### Administering data access applications on Liberty

With Liberty, applications can access data in both relational and NoSQL databases.

#### Procedure

- Configuring relational database connectivity in Liberty.
- Configure connection pooling for database connections
- Configure database transaction recovery

#### Configuring relational database connectivity in Liberty:

You can configure a data source associated with different JDBC providers for database connectivity. The JDBC providers supply the driver implementation classes that are required for JDBC connectivity with your specific vendor database.

#### About this task

To access a database from your application, you must use a data source. Data sources are provided by JDBC drivers and come in the following varieties:

- `javax.sql.DataSource`  
This is the basic form of a data source. It does not provide interoperability that enhances connection pooling, and cannot participate as a two-phase capable resource in transactions involving multiple resources.
- `javax.sql.ConnectionPoolDataSource`  
This type of data source is enabled for connection pooling. It cannot participate as a two-phase capable resource in transactions involving multiple resources.
- `javax.sql.XADataSource`  
This type of data source is both enabled for connection pooling and is able to participate as a two-phase capable resource in transactions involving multiple resources.

In order to be usable in the Liberty, your JDBC driver must provide at least one of these types of data sources. For the commonly used JDBC drivers, Liberty is already aware of the implementation class names for the various data source types. You only need to tell Liberty where to find the JDBC driver.

#### Procedure

1. In the `server.xml` file, define a shared library pointing to the location of your JDBC driver JAR or compressed files. For example:

```
<library id="DB2JCC4Lib">
  <fileset dir="C:/DB2/java" includes="db2jcc4.jar db2jcc_license_cisuz.jar"/>
</library>
```

2. Define a data source using the JDBC driver. If you don't specify the type of data source, Liberty chooses the data source in the following order depending on which is available.

- javax.sql.ConnectionPoolDataSource
- javax.sql.DataSource
- javax.sql.XADataSource

Here is an example that accepts the default for data source type:

```
<dataSource id="db2" jndiName="jdbc/db2">
  <jdbcDriver libraryRef="DB2JCC4Lib"/>
  <properties.db2.jcc databaseName="SAMPLEDB" serverName="localhost" portNumber="50000"/>
</dataSource>
```

Here is an example that uses javax.sql.XADataSource type:

```
<dataSource id="db2xa" jndiName="jdbc/db2xa" type="javax.sql.XADataSource">
  <jdbcDriver libraryRef="DB2JCC4Lib"/>
  <properties.db2.jcc databaseName="SAMPLEDB" serverName="localhost" portNumber="50000"/>
</dataSource>
```

A default data source is available when at least one Java EE 7 feature is enabled. This data source uses a different priority to determine the type if none is specified.

- javax.sql.XADataSource
- javax.sql.ConnectionPoolDataSource
- javax.sql.DataSource

This data source is available as java:comp/DefaultDataSource. A jndiName does not need to be specified for it. To configure the default data source, specify a data source with the id set to DefaultDataSource. Here is an example that configures the default data source to point at a DB2 database:

```
<dataSource id="DefaultDataSource">
  <jdbcDriver libraryRef="DB2JCC4Lib"/>
  <properties.db2.jcc databaseName="SAMPLEDB" serverName="localhost" portNumber="50000"/>
</dataSource>
```

3. Optional: Configure attributes for the data source, such as JDBC vendor properties and connection pooling properties.

For example:

```
<dataSource id="DefaultDataSource" jndiName="jdbc/db2" connectionSharing="MatchCurrentState"
  isolationLevel="TRANSACTION_READ_COMMITTED" statementCacheSize="20">
  <connectionManager maxPoolSize="20" minPoolSize="5"
    connectionTimeout="10s" agedTimeout="30m"/>
  <jdbcDriver libraryRef="DB2JCC4Lib"/>
  <properties.db2.jcc databaseName="SAMPLEDB" serverName="localhost" portNumber="50000"
    currentLockTimeout="30s" user="user1" password="pwd1"/>
</dataSource>
```

For a full list of configuration attributes for the dataSource element, connectionManager element and some commonly used JDBC vendors, see “Data Source (dataSource)” on page 191.

4. Optional: Configure data sources for commonly used databases according to the following examples.

#### For DB2

```
<dataSource id="DefaultDataSource" jndiName="jdbc/db2">
  <jdbcDriver libraryRef="DB2JCC4Lib"/>
  <properties.db2.jcc databaseName="SAMPLEDB" serverName="localhost" portNumber="50000"/>
</dataSource>

<library id="DB2JCC4Lib">
  <fileset dir="C:/DB2/java" includes="db2jcc4.jar db2jcc_license_cisuz.jar"/>
</library>
```

### For DB2 on iSeries (Native)

```
<dataSource id="DefaultDataSource" jndiName="jdbc/db2iNative">
  <jdbcDriver libraryRef="DB2iNativeLib"/>
  <properties.db2.i.native databaseName="*LOCAL"/>
</dataSource>

<library id="DB2iNativeLib">
  <fileset dir="/QIBM/Proddata/java400/jdk6/lib/ext" includes="db2_classes16.jar"/>
</library>
```

### For DB2 on iSeries (Toolbox)

```
<dataSource id="DefaultDataSource" jndiName="jdbc/db2iToolbox">
  <jdbcDriver libraryRef="DB2iToolboxLib"/>
  <properties.db2.i.toolbox databaseName="SAMPLEDB" serverName="localhost"/>
</dataSource>

<library id="DB2iToolboxLib">
  <fileset dir="/QIBM/ProdData/Http/Public/jt400/lib" includes="jt400.jar"/>
</library>
```

### For Derby Embedded

```
<dataSource id="DefaultDataSource" jndiName="jdbc/derbyEmbedded">
  <jdbcDriver libraryRef="DerbyLib"/>
  <properties.derby.embedded databaseName="C:/databases/SAMPLEDB" createDatabase="create"/>
</dataSource>

<library id="DerbyLib">
  <fileset dir="C:/db-derby-10.8.1.2-bin/lib"/>
</library>
```

### For Derby Network Client

```
<dataSource id="DefaultDataSource" jndiName="jdbc/derbyClient">
  <jdbcDriver libraryRef="DerbyLib"/>
  <properties.derby.client databaseName="C:/databases/SAMPLEDB" createDatabase="create"
    serverName="localhost" portNumber="1527"/>
</dataSource>

<library id="DerbyLib">
  <fileset dir="C:/db-derby-10.8.1.2-bin/lib"/>
</library>
```

### For Informix® JCC

```
<dataSource id="DefaultDataSource" jndiName="jdbc/informixjcc">
  <jdbcDriver libraryRef="DB2JCC4Lib"/>
  <properties.informix.jcc databaseName="SAMPLEDB" serverName="localhost" portNumber="1526"/>
</dataSource>

<library id="DB2JCC4Lib">
  <fileset dir="C:/Drivers/jcc/4.8" includes="db2jcc4.jar db2jcc_license_cisuz.jar"/>
</library>
```

### For Informix JDBC

```
<dataSource id="DefaultDataSource" jndiName="jdbc/informix">
  <jdbcDriver libraryRef="InformixLib"/>
  <properties.informix databaseName="SAMPLEDB" ifxIFXHOST="localhost"
    serverName="ol_machinename" portNumber="1526"/>
</dataSource>

<library id="InformixLib">
  <fileset dir="C:/Drivers/informix" includes="ifxjdbc.jar ifxjdbcx.jar"/>
</library>
```

### For Microsoft SQL Server (Microsoft JDBC driver)

```
<dataSource id="DefaultDataSource" jndiName="jdbc/mssqlserver">
  <jdbcDriver libraryRef="MSJDBClib"/>
  <properties.microsoft.sqlserver databaseName="SAMPLEDB"
    serverName="localhost" portNumber="1433"/>
</dataSource>
```

```

<library id="MSJDBClib">
  <fileset dir="C:/sqljdbc_6.0/enu/sqljdbc41.jar"/>
</library>

```

#### For Microsoft SQL Server (DataDirect Connect for JDBC driver)

```

<dataSource id="DefaultDataSource" jndiName="jdbc/ddsqserver">
  <jdbcDriver libraryRef="DataDirectLib"/>
  <properties.datadirect.sqlserver databaseName="SAMPLEDB"
    serverName="localhost" portNumber="1433"/>
</dataSource>

<library id="DataDirectLib">
  <fileset dir="C:/DataDirect/Connect-4.2/lib/sqlserver.jar"/>
</library>

```

#### For MySQL

```

<dataSource id="DefaultDataSource" jndiName="jdbc/mysql">
  <jdbcDriver libraryRef="MySQLLib"/>
  <properties databaseName="SAMPLEDB" serverName="localhost" portNumber="3306"/>
</dataSource>

<library id="MySQLLib">
  <fileset dir="C:/mysql-connector-java-x.x.xx/mysql-connector-java-x.x.xx.jar"/>
</library>

```

#### For Oracle

```

<dataSource id="DefaultDataSource" jndiName="jdbc/oracle">
  <jdbcDriver libraryRef="OracleLib"/>
  <properties.oracle URL="jdbc:oracle:thin:@//localhost:1521/SAMPLEDB"/>
</dataSource>

<library id="OracleLib">
  <fileset dir="C:/Oracle/lib/ojdbc6.jar"/>
</library>

```

#### For Sybase

```

<dataSource id="DefaultDataSource" jndiName="jdbc/sybase">
  <jdbcDriver libraryRef="SybaseLib"/>
  <properties.sybase databaseName="SAMPLEDB" serverName="localhost" portNumber="5000"/>
</dataSource>

<library id="SybaseLib">
  <fileset dir="C:/Drivers/sybase/jconn4.jar"/>
</library>

```

#### For solidDB

```

<dataSource id="DefaultDataSource" jndiName="jdbc/solidDB">
  <jdbcDriver libraryRef="solidLib"/>
  <properties databaseName="SAMPLEDB" URL="jdbc:solid://localhost:2315"/>
</dataSource>

<library id="solidLib">
  <fileset dir="C:/Drivers/solidDB/SolidDriver2.0.jar"/>
</library>

```

#### For a JDBC driver that is not known to Liberty

```

<dataSource id="DefaultDataSource" jndiName="jdbc/sample" type="javax.sql.XADataSource">
  <jdbcDriver libraryRef="SampleJDBClib"
    javax.sql.XADataSource="com.ibm.sample.SampleXADataSource"/>
  <properties databaseName="SAMPLEDB" hostName="localhost" port="12345"/>
</dataSource>

<library id="SampleJDBClib">
  <fileset dir="C:/Drivers/SampleJDBC/sampleDriver.jar"/>
</library>

```

In the example, the JDBC driver is located at C:/Drivers/SampleJDBC/sampleDriver.jar and provides an implementation of javax.sql.XADataSource named

com.ibm.sample.SampleXADDataSource. The JDBC driver also provides vendor-specific data source properties such as **databaseName**, **hostName** and **port**.

Configuring a default data source: 8.5.5.6

You can configure a default data source that is associated with different JDBC providers for database connectivity. The JDBC providers supply the driver implementation classes that are required for JDBC connectivity with your specific vendor database.

### About this task

To access a database from your application, you must configure a data source.

### Procedure

1. Configure the `datasource` element with the ID `DefaultDataSource` in the `server.xml` file.

```
<dataSource id="DefaultDataSource">
  <jdbcDriver libraryRef="MyJDBCLib"/>
  <properties.derby.embedded databaseName="myDB" createDatabase="create"/>
  <containerAuthData user="user1" password="{xor}0z0vKDtu" />
</dataSource>
<library id="MyJDBCLib">
  <file name="C:/derby/derby.jar"/>
</library>
```

**Note:** The server must be running at the Java Enterprise Edition 7 platform level. This platform level is enabled when one or more Java Enterprise Edition 7 features are enabled in the `server.xml` file.

2. To use the `DefaultDataSource` in a web application, a reference can be obtained with dependency injection:

```
@Resource
DataSource defaultDataSource;
```

or through JNDI lookup:

```
DataSource defaultDataSource = (DataSource) new InitialContext().lookup("java:comp/DefaultDataSource");
```

*Liberty:How data source configuration updates are applied:*

If you change the attributes of the **dataSource** element while a server is running, the updates to different attributes are applied at different times and in different ways.

You configure a data source by specifying the attributes of the **dataSource** element in the `server.xml` configuration file. If you change these attributes for a running server, the updates are applied at different times and in different ways, depending on which attribute is changed. The following table describes, for each attribute of the **dataSource** element, how a configuration change is applied at run time.

*Table 120. How data source configuration updates are applied at run time.* The first column of the table lists the attributes of the **dataSource** element. The second column describes, for each attribute, how the configuration update is applied at run time.

Attribute name	How the configuration update is applied
<b>beginTranForResultSetScrollingAPIs</b>	The update is effective immediately.
<b>beginTranForVendorAPIs</b>	The update is effective immediately.
<b>commitOrRollbackOnCleanup</b>	The update is effective immediately.
<b>connectionManagerRef</b>	All connections and the connection pool are destroyed. The data source is then managed by the new connection manager.
<b>connectionSharing</b>	The update is applied with each first connection handle in a transaction.

Table 120. How data source configuration updates are applied at run time (continued). The first column of the table lists the attributes of the `dataSource` element. The second column describes, for each attribute, how the configuration update is applied at run time.

Attribute name	How the configuration update is applied
<code>isolationLevel</code>	The update is applied with new connection requests; current connections retain their isolation level.
<code>jdbcDriverRef</code>	All connections and the connection pool are destroyed. The new JDBC driver is then used.
<code>jndiName</code>	All connections and the connection pool are destroyed. The new JNDI name is then used.
<code>propertiesRef</code>	If the data source is Derby Embedded, all connections and the connection pool are destroyed before new properties go into effect. For other JDBC drivers, the new properties go into effect with new connection requests.
<code>queryTimeout</code>	The update is effective immediately.
<code>recoveryAuthDataRef</code>	Authentication data for transaction recovery. All connections and the connection pool are destroyed. The new recovery authentication data is then used.
<code>statementCacheSize</code>	The statement cache is resized upon next use.
<code>supplementalJDBCTrace</code>	All connections and the connection pool are destroyed. The new setting is then used.
<code>syncQueryTimeoutWithTransactionTimeout</code>	The update is effective immediately.
<code>transactional</code>	The update is applied to new connections and existing connections not in use from the connection pool.
<code>type</code>	All connections and the connection pool are destroyed. The new setting is then used.

*Liberty:Application-defined data sources:*

You can define a data source within your application, through annotations or in the deployment descriptor, as defined by the Java EE specification.

**Note:** **8.5.5.0** The `commonLibraryRef` class loader attribute is recommended for application defined data sources. The `privateLibraryRef` attribute cannot be used for the `java:global` namespace and is discouraged for the other scopes. If multiple applications declare the same `java:global` namespace to specify the data source, the `server.xml` files of the applications must all specify a `commonLibraryRef` attribute to the same shared library.

When defining a data source in an application, the JDBC driver must be made available to the application. This is accomplished by configuring a shared library in the `server.xml` for your application.

For example:

```
<application id="myApp" name="myApp" location="myApp.war" type="war">
  <classloader commonLibraryRef="DB2Lib"/>
</application>

<library id="DB2Lib">
  <fileset dir="C:/DB2/java" includes="db2jcc4.jar db2jcc_license_cisuz.jar"/>
</library>
```

Then, you can define a data source in your application either through annotations or in the deployment descriptor.

- Use annotations as in the following example:

```

@DataSourceDefinition(
    name           = "java:comp/env/jdbc/db2",
    className      = "com.ibm.db2.jcc.DB2DataSource",
    databaseName   = "SAMPLEDB",
    serverName     = "localhost",
    portNumber     = 50000,
    properties     = { "driverType=4" },
    user           = "user1",
    password       = "pwd1"
)

```

```

public class MyServlet extends HttpServlet {

    @Resource(lookup="java:comp/env/jdbc/db2")
    DataSource ds;

```

- Use the deployment descriptor as in the following example, for example, in a web.xml file:

```

<data-source>
  <name>java:comp/env/jdbc/db2</name>
  <class-name>com.ibm.db2.jcc.DB2DataSource</class-name>
  <server-name>localhost</server-name>
  <port-number>50000</port-number>
  <database-name>SAMPLEDB</database-name>
  <user>user1</user>
  <password>pwd1</password>
  <property><name>driverType</name><value>4</value></property>
</data-source>

```

In general, properties that can be defined on `dataSource` or `connectionManager` in the `server.xml` files can also be specified on application defined data sources. Two exceptions to this are `connectionManagerRef` and `jdbcDriverRef`, which you cannot specify because the application defined data source implicitly defines the connection manager and JDBC driver. When using application defined data sources for two-phase commit, you can specify the `recoveryAuthDataRef` property to select the authentication data that is used for transaction recovery. However, it is important to be aware that recovery of transactions is only possible while the application is running. You can use variables, encoded passwords, and duration syntax in application defined data sources.

**Note:** The duration syntax does not apply to properties that are explicitly defined in the annotation, such as `loginTimeout` or `maxIdleTime`.

Here is an example of two data sources using connection manager properties, variables, encoded passwords, and duration syntax.

```

@DataSourceDefinitions(value = {
    @DataSourceDefinition(
        name           = "java:comp/env/jdbc/derby",
        className      = "org.apache.derby.jdbc.EmbeddedDataSource40",
        databaseName   = "${shared.resource.dir}/data/SAMPLEDB",
        minPoolSize    = 1,
        maxPoolSize    = 10,
        maxIdleTime    = 180,
        properties     = { "agedTimeout=10m", "connectionTimeout=30s", "createDatabase=create" }
    ),
    @DataSourceDefinition(
        name           = "java:comp/env/jdbc/oracle",
        className      = "oracle.jdbc.pool.OracleDataSource",
        url            = "jdbc:oracle:thin:@//localhost:1521/SAMPLEDB",
        user           = "user1",
        password       = "{xor}0z0vKDtt"
    )
})

```

You can use the client reroute feature to configure your enterprise applications for a DB2 database to recover from a communication loss, and the applications can continue to work with minimal interruption. Rerouting is central to the support of continuous operations, but rerouting is only possible when there is an alternative location that is identified to the application server connection.

### Before you begin

This task assumes that:

- The DB2 data source to which your application connects is running:
  - DB2 for z/OS Version 10.1 or later or
  - DB2 Database for Linux, UNIX, and Windows Version 9.7 or later
- You configured the DB2 database with a redundant setup or the ability to fail the DB2 server to a standby node.

### About this task

You can use client reroute for DB2 to provide information about alternative servers in case the connection to the primary database server fails.

Without any configuration on the client side, the Java Common Connectivity (JCC) Java Database Connectivity (JDBC) driver for DB2 supports the client reroute capability, if it is enabled on the DB2 server, when the driver makes an initial connection to the DB2 server. When the JCC JDBC driver connects to a DB2 server that has one or more alternative servers that are configured, the primary server sends information about the alternative servers to the JCC JDBC driver. If the connection to the primary server fails, the JCC JDBC driver is able to reroute connections to an alternative server. If the application server process crashes, however, the alternative server information is lost and the client needs to connect to the primary server again. If the client cannot make an initial connection to the primary server, the client has no knowledge of the alternative servers and cannot reroute.

To overcome this problem, you can configure a DB2 data source in the application server with the **Alternate server name** and **Alternate port number** fields, or with the `clientRerouteAlternateServerName` and `clientRerouteAlternatePortNumber` data source custom properties, to support client reroute even on the initial connection attempt. If the JDBC driver is not able to connect to the primary DB2 server, the information that is necessary for a client reroute is already present, and the JDBC driver can reroute the connection to an alternate server.

**Attention:** The data source custom property, `enableClientAffinitiesList`, changes the semantics of the `clientRerouteAlternateServerName` and `clientRerouteAlternatePortNumber` properties.

When a connection is rerouted and the JCC JDBC driver is connected to the alternative DB2 server, the alternative server sends information about its own alternative server to the JCC JDBC driver. The JCC JDBC driver then has the information that is required to reroute the connection again if the alternative DB2 server is not available. The server that was originally the alternative server is now the primary server, and a new alternative server is established. However, this new state of the primary and alternative servers is no longer kept by the JCC JDBC driver. If the application server fails and is restarted, the JCC JDBC driver must start from the original server configuration and attempt to connect to the server that was originally considered the primary server.

You can use the automatic client rerouting feature within the following DB2 configurable environments:

- Enterprise Server Edition (ESE) with the data partitioning feature (DPF)
- Data Propagator (DPROPR)-style replication
- High availability cluster multiprocessor (HACMP<sup>™™</sup>)

- High availability disaster recovery (HADR)

## Procedure

1. Define your DB2 data source in the `server.xml` file with the following properties:

- `clientRerouteAlternateServerName`
  - Type of valid values:
    - Domain name; for example: `www.ibm.com`
    - IP address (IPv4 and IPv6); for example: `23.72.11.219`
  - Format of multiple values:
    - Comma separated; for example: `host1, host2, host3`
    - Space separated; for example: `host1 host2 host3`
  - Order significance:
    - The order of the provided host names is the order that the JCC JDBC driver uses to try to find the next available server to connect to.
- `clientRerouteAlternatePortNumber`
  - Type of valid values:
    - Integer representing the port number; for example: `50000`
  - Format of multiple values:
    - Comma separated; for example: `port1, port2, port3`
    - Space separated; for example: `port1 port2 port3`
  - Order significance:
    - The order of the provided ports must match the order of their associated servers.

2. (Optional) You can add one or both of the following properties:

- `retryIntervalForClientReroute`

This property defines the number of seconds the JCC JDBC driver waits between each attempt to establish a connection.

If no value is assigned, the default behavior is used. To learn more, see [JDBC and SQL support](#).
- `maxRetriesForClientReroute`

This property defines the number of retries the JCC JDBC driver attempts to connect the server before it decides to move on to the next server. This property is only used when `RetryIntervalForClientReroute` property is set.

If no value is assigned, the default behavior is used. To learn more, see [JDBC and SQL support](#).

## Example

```
<dataSource id="DefaultDataSource"jndiName="jdbc/db2">
  <properties.db2.jcc
    databaseName="sampleDatabase"
    driverType="4"
    serverName="host"
    portNumber="50000"
    clientRerouteAlternateServerName="host01, host02, host03"
    clientRerouteAlternatePortNumber="50000, 50005, 50000"
    retryIntervalForClientReroute="2"
    maxRetriesForClientReroute="3" />
  ...
</dataSource>
```

**Note:** Ensure that an equal number of entries is specified for both ports and hosts. Otherwise, a warning is displayed and client reroute is not enabled.

The Liberty server can be enabled to interact with DB2 by using the JDBC Type 2 driver implementation on z/OS.

## Before you begin

The angel process must be started before you enable this support. For more information, see “Administering Liberty on z/OS” on page 1731. You can configure a Liberty Profile server to run as a z/OS started task. For more information, see [Configuring a Liberty Profile server as a z/OS started task](#).

## About this task

When you use an RRS capable resource such as DB2, you have the following optional configurations:

- You can enable the server to automatically delete resource manager names from the Resource and Recovery Services (RRS) RM.DATA logstream when the server is stopped. This configuration is optional, but if enabled it prevents resource manager names from accumulating in the logstream. To enable automatic RM name deletion, configure Resource Access Control Facility (RACF) to allow the server to call the ATRSRV macro. To enable automatic RM name deletion, the user ID that the Liberty server runs under must have ALTER access in the FACILITY class to either:
  - MVSADMIN.RRS.COMMANDS.gname.sysname resource to access to a specific logging group name (gname) and system (sysname)
  - MVSADMIN.RRS.COMMANDS.\* resource to allow access to all systems and logging group names
- You can define the RM.METADATA logstream to log data that assists debugging. The user ID that the Liberty server runs under must have ALTER access in the FACILITY class as described.

**Note:** For more information about the ATRSRV macro, setting the appropriate RACF permission, and how to define the RM.METADATA logstream, refer to the *MVS Programming: Resource Recovery* publication relevant to your system's z/OS level.

- You can control the time to wait for transactions actively by using native contexts to complete when the server is stopped or the `zosTransaction-1.0` feature is no longer needed. This can be done by using `nativeTransactionManager` configuration element and the `shutdownTimeout` attribute.
- You can restrict user authority for performing any transactional work that involves RRS capable resources, for example DB2 T2, on a particular server. This can be done by using `nativeTransactionManager` configuration element, and the `resourceManagerNamePrefix` attribute.

**Note:** The `resourceManagerNamePrefix` attribute specifies a 1-8 alphanumeric (A-Z, a-z, 0-9) and national (@,#,\$) only character prefix to be used as part of the server generated resource manager name that is registered with RRS. The prefix "DEFAULT" is a reserved prefix that identifies a default server configuration and should not be used for securing server access. If the configured prefix does not follow the name, length, and character requirements, the DEFAULT prefix name is used. The prefix is intended for system administrators to enable only authorized users to perform transactional work (normal and recovery) involving RRS capable resources. For example DB2 T2, on the server where the prefix was configured. System administrators must define a `BBG.RMNAME.<PREFIX>.RRS` resource under the SERVER class, and give the required users READ authority.

These examples describe the optional configuration:

Server.xml element and attribute definition:

```
<nativeTransactionManager shutdownTimeout="20s" resourceManagerNamePrefix="PROD1"/>
```

RACF resource definition and user authorization:

```
RDEF SERVER BBG.RMNAME.PROD1.RRS UACC(NONE)
PERMIT BBG.RMNAME.PROD1.RRS CLASS(SERVER) ACCESS(READ) ID(PROD1USR)
SETR RACLIST(SERVER) GENERIC(SERVER) REFR
```

## Procedure

1. Update the Liberty server's `server.xml` configuration file. Add the `zosTransaction-1.0` feature subelement to the `featureManager` element:

```
<featureManager>
  <feature>zosTransaction-1.0</feature>
</featureManager>
```

Specifying this feature enables the application server to synchronize and appropriately manage transactional activity between the Resource Recovery Services (RRS), the transaction manager of the application server, and the resource manager. So, work without configuring the `zosTransaction-1.0` feature is not allowed.

2. Add the resource's (DB2) native libraries to the resource's `<library>` configuration element: The `<library>` element in the example shows:

```
<library id="DB2T2LibRef">
  <fileset dir="<YOUR DB2 T2 LIBRARY PATHS>" />
  <fileset dir="<YOUR DB2 T2 NATIVE LIBRARY PATHS>" />
</library>
```

3. Configure the `jdbcDriver` and `datasource` elements.

When you define the `datasource` element, you can skip configuring the `type` attribute because the value `javax.sql.ConnectionPoolDataSource` is used by default. If you choose to explicitly configure the `type` attribute, you must use the value: `javax.sql.ConnectionPoolDataSource`.

The `datasource` element can include a child element named `properties.db2.jcc`. Attributes that are supplied in the `properties.db2.jcc` element are passed directly to the DB2 JCC Driver. The `driverType` attribute is required and must be set to 2. The `databaseName` attribute is also required. The `ssid` attribute is not required, but can be used to control which DB2 for z/OS subsystem this data source connects to if there are multiple DB2 subsystems on the LPAR.

## Example

This example describes how to configure your application, jdbc driver, library, fileset, and data source elements, in the `server.xml` configuration file.

```
<application type="war" id="db2T2TxWar" name="db2T2TxWar"
  location="/u/user1/wlp/usr/servers/defaultServer/dropins/db2T2Tx.war" />
<jdbcDriver id="DB2T2" libraryRef="DB2T2LibRef"/>

<library id="DB2T2LibRef">
  <fileset dir="/db2v10/jcc/classes" />
  <fileset dir="/db2v10/jcc/lib" />
</library>

<dataSource id="jdbc/DB2T2" jndiName="jdbc/DB2T2" jdbcDriverRef="DB2T2">
  <properties.db2.jcc driverType="2" databaseName="LOC1" />
</dataSource>
```

*Configuring connection pooling for database connections:*

You can configure connection pooling for your data source by defining a connection manager for it.

## Example

The following example code uses the `connectionManager` element in the `server.xml` file to define a connection pool for a data source:

```
<dataSource id="DefaultDataSource" jndiName="jdbc/example" jdbcDriverRef="DB2" >
  <connectionManager maxPoolSize="10" minPoolSize="2"/>
  <properties.db2.jcc databaseName="TESTDB"/>
</dataSource>
```

The server uses default values for any connection management settings that are not defined on the connection manager element. If a connection manager is not defined at all for a data source, the server uses default values for all of the settings.

Using thread local storage for connections can increase performance for applications on multi-threaded systems. See Chapter 12, “Tuning Liberty,” on page 2291.

You can define multiple data sources and associate each with a different connection manager. However, you cannot associate multiple data sources with a single connection manager.

For more information about the `connectionManager` element, see .

*Liberty:How connection pooling configuration updates are applied:*

If you change the attributes of the **connectionManager** element while a server is running, the updates to different attributes are applied at different times and in different ways.

You configure a connection pool by specifying the attributes of the **connectionManager** element in the `server.xml` configuration file. If you change these attributes for a running server, the updates are applied at different times and in different ways, depending on which attribute is changed. The following table describes, for each attribute of the **connectionManager** element, how a configuration change is applied at run time.

*Table 121. How connection manager configuration updates are applied at run time.* The first column of the table lists the attributes of the **connectionManager** element. The second column describes, for each attribute, how the configuration update is applied at run time.

Attribute name	How the configuration update is applied
<b>agedTimeout</b>	The update is effective immediately.
<b>connectionTimeout</b>	The update is effective immediately.
<b>maxIdleTime</b>	The update is effective immediately.
<b>maxNumberOfMCsAllowableInThread</b>	The update is effective immediately.
<b>maxPoolSize</b>	The update is effective immediately.
<b>minPoolSize</b>	The update is effective immediately.
<b>numConnectionsPerThreadLocal</b>	The update is effective immediately.
<b>reapTime</b>	The update is effective immediately.
<b>purgePolicy</b>	The update is effective immediately.

**Note:** The attributes **agedTimeout** and **maxIdleTime** are updated immediately. However, they are not used fully unless the value of **reapTime** attribute is greater than zero.

Because updates to the connection manager are effective immediately, errors might occur if you make changes with active connections; including the potential risks for the connections to be ended prematurely.

### Configuring MongoDB connectivity in Liberty: **8.5.5.0**

Applications that use MongoDB can run on Liberty. For access to a MongoDB instance, the applications use the MongoDB Java driver and data sources that you configure for the server.

#### Before you begin

**Note:** **8.5.5.0** The Liberty provides configuration support for MongoDB. MongoDB (from “humongous”) is a scalable, high-performance, open source NoSQL database.

Only MongoDB Java driver versions 2.10.0 to 2.12.5 are supported.

## About this task

To enable an application to use MongoDB, you configure a shared library for the MongoDB Java driver and a library reference to the shared library in the `server.xml` file of Liberty. An application can access MongoDB directly from the application or through the `mongodb-2.0` feature and MongoDB instance configurations in the `server.xml` file.

## Procedure

1. Install the MongoDB Java driver in a location that your application and the Liberty runtime can access.

For example, place the MongoDB driver `.jar` file in the `Liberty_profile_root/usr/servers/server_name/lib` directory.

2. Configure a shared library for the MongoDB driver `.jar` file in the `server.xml` file of the Liberty server.

```
<library id="MongoLib">
  <file name="{server.config.dir}/lib/mongo.jar" />
</library>
```

3. Enable your application to access MongoDB, either by direct access from the application or by using the `mongodb-2.0` feature.

- Enable direct access to MongoDB from the application.
  - a. Configure a library reference for the shared library in an application element in the `server.xml` file.

```
<application ...>
  <classloader commonLibraryRef="MongoLib"/>
</application>
```

The application can now access the MongoDB APIs directly. If you want the application to use the runtime injection engine, continue with the next steps.

- Configure the `mongodb-2.0` feature, `mongo`, and `mongoDB` elements in the `server.xml` file.
  - a. Add the `mongodb-2.0` feature to the `server.xml` file.

```
<featureManager>
  <feature>mongodb-2.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>
```

The JNDI feature is only required when you use `jndi` to look up resources. It is not required if you use resource injection.

- b. Configure a `mongo` element that has a reference to the shared library created in a previous step.

```
<mongo id="mongo" libraryRef="MongoLib" />
```

- c. Configure the `mongoDB` element.

```
<mongoDB jndiName="mongo/testdb" mongoRef="mongo" databaseName="db-test" />
```

Configuring a JNDI name enables an application or the Liberty runtime to look up the MongoDB instance.

- d. Enable your application to access MongoDB.

The following example shows both JNDI lookup and resource injection:

```
public class TestServlet extends HttpServlet {
    @Resource(name = "mongo/testdb")
    protected DB db;
    ...
    protected void doGet(HttpServletRequest request,
        HttpServletResponse response) throws ServletException, IOException {
        // Alternatively use InitialContext lookup
        DB lookup = (DB) new InitialContext().lookup("java:comp/env/mongo/testdb");
        ...
    }
}
```

- e. If you are using JNDI lookup, add a resource environment reference to the `web.xml` file of your application:

```
<resource-env-ref>
  <resource-env-ref-name>mongo/testdb</resource-env-ref-name>
  <resource-env-ref-type>com.mongodb.DB</resource-env-ref-type>
</resource-env-ref>
```

## What to do next

Test use of the MongoDB from your application.

Optionally, review additional configuration properties in the `mongo` and `mongoDB` sections of .

*Configuring secure MongoDB connections in Liberty:* **8.5.5.0**

You can configure application-managed or container-managed security for MongoDB connections in Liberty.

## Before you begin

Enable your application to use MongoDB. See [Creating Liberty applications that use MongoDB](#).

## About this task

You can secure MongoDB applications by using application-managed security or container-managed security. For both types of security, the MongoDB server must be running with authentication explicitly enabled to secure MongoDB connections.

## Procedure

- Configure application-managed security for MongoDB.

If the `mongo` configuration element does not specify user and password attributes, the product assumes that an application is either using application-managed security or is not using security. To enable application-managed security, the application must authenticate using the MongoDB APIs; for example:

```
<mongo id="mongo1" libraryRef="MongoLib" />
<mongoDB jndiName="mongo/testdb" mongoRef="mongo1" databaseName="db-test-1"/>
```

```
{ ...
// Java snippet
@Resource(name = "mongo/testdb")
protected DB db;

private void auth() {
  if (!db.isAuthenticated())
    db.authenticate("user", "password".toCharArray());
}
```

- Configure container-managed security for MongoDB.

To use container-managed security, the `mongo` configuration element must specify a user and password. Only one user is allowed for each `mongo` configuration. All MongoDB instances use the specified user and password. For example, all MongoDB instances that reference `mongo1` in the following example use `mongoUserName` and `pw`:

```
<mongo id="mongo1" libraryRef="MongoLib" user="mongoUserName" password="pw"/>
<mongoDB jndiName="mongo/testdb" mongoRef="mongo1" databaseName="db-test-1"/>
<mongoDB jndiName="mongo/testdb2" mongoRef="mongo1" databaseName="db-test-2"/>
```

Applications that use container-managed security must not call `com.mongodb.DB.authenticate(user, pass)`.

## What to do next

Ensure that the MongoDB server is running, and then test the MongoDB security from your application.

Connecting to a distributed set of MongoDB instances: **8.5.5.0**

Accessing data that is stored in a distributed set of MongoDB instances is nearly the same procedure as connecting to a single MongoDB instance.

## Before you begin

Enable your application to use MongoDB. See [Creating Liberty applications that use MongoDB](#).

## About this task

When you configure the mongo feature in your `server.xml` file, you can pass a collection of `hostNames` and ports that are either replica set members or sharded mongos servers.

If the `host:port` combinations are replica set members, the client finds all members and uses the master by default. If the combinations are sharded mongos servers, the client sends all requests to the closest member with the lowest ping time. If the closest member is down, the client automatically fails over to the next server.

## Procedure

Configure the `hostNames` and ports in your `server.xml` file.

```
<mongo id="mongo1" libraryRef="MongoLib" hostNames="localhost,localhost,localhost" ports="9991,9992,9993"/>
```

## Results

You configured a sharded MongoDB configuration.

Configuring CouchDB connectivity with the ektorp client library in Liberty: **8.5.5.4**

Applications that run on Liberty can use CouchDB. For access to a CouchDB instance, applications can configure a connector for the NoSQL database with the ektorp client library.

## Before you begin

Liberty provides configuration support for CouchDB. CouchDB is a scalable, high-performance, open source NoSQL database.

You must use Version 1.4.1 or later of the ektorp Java driver. Use the Maven plug-in to obtain the ektorp driver and its dependencies.

```
<dependency>
  <groupId>org.ektorp</groupId>
  <artifactId>org.ektorp</artifactId>
  <version>1.4.1</version>
</dependency>
```

## About this task

To enable an application to use CouchDB, you must configure a shared library for the CouchDB Java driver and a library reference to the shared library in the `server.xml` file. An application can access CouchDB either directly from the application, or through the `couchdb-1.0` feature and CouchDB instance configurations in the `server.xml` file.

## Procedure

1. Install the CouchDB Java driver in a location that your application and the Liberty runtime can access. For example, place the ektorp driver file and its dependencies in the `Liberty_profile_root/usr/servers/server_name/lib` directory.
2. Configure a shared library for the ektorp driver files in the `server.xml` file of the Liberty server.

```
<library id="couchdb-lib">
  <fileset
    dir='${server.config.dir}/lib'
    includes='org.ektorp-1.4.1.jar
    commons-codec-1.6.jar
    commons-io-2.0.1.jar
    commons-logging-1.1.1.jar
    httpclient-4.2.5.jar
    httpclient-cache-4.2.5.jar
    httpcore-4.2.4.jar
    jackson-annotations-2.2.2.jar
    jackson-core-2.2.2.jar
    jackson-databind-2.2.2.jar
    slf4j-api-1.6.4.jar
    slf4j-simple-1.6.4.jar' />
</library>
```

3. Enable your application to access CouchDB, either by direct access from the application or by using the `couchdb-1.0` feature.

- Enable direct access to CouchDB from the application.
  - a. Configure a library reference for the shared library in an application element in the `server.xml` file.

```
<application ...>
  <classloader commonLibraryRef="couchdb-lib"/>
</application>
```

The application can now access the CouchDB APIs directly. If you want the application to use the runtime injection engine, continue with the next steps.

- Configure the `couchdb-1.0` feature, and the `couchdb` elements in the `server.xml` file.
  - a. Add the `couchdb-1.0` feature to the `server.xml` file.

```
<featureManager>
  <feature>couchdb-1.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>
```

The JNDI feature is only required when you use JNDI to look up resources. This feature is not required if you use resource injection.

- b. Configure a `couchdb` element that has a reference to the shared library created in a previous step.

```
<couchdb id="couchdb" jndiName="couchdb/connector"
  libraryRef="couchdb-lib" url="http://example.com:5984" username="username"
  password="password"/>
```

Configuring a JNDI name enables an application or the Liberty runtime to look up the CouchDB instance.

- c. Enable your application to access CouchDB.

The following example shows both JNDI lookup and resource injection:

```
public class TestServlet extends HttpServlet {
    @Resource(name = "couchdb/connector")
    protected CouchDbInstance db;
    ...
    protected void doGet(HttpServletRequest request,
        HttpServletResponse response) throws ServletException, IOException {
```

```
// Alternatively use InitialContext lookup
    CouchDbInstance lookup = (CouchDbInstance) new
InitialContext().lookup("java:comp/env/couchdb/connector");
...

```

- d. If you are using JNDI lookup, add a resource environment reference to the `web.xml` file of your application:

```
<resource-env-ref>
  <resource-env-ref-name>couchdb/connector</resource-env-ref-name>
  <resource-env-ref-type>org.ektorp.CouchDbInstance</resource-env-ref-type>
</resource-env-ref>

```

You can use the `couchdb-1.0` feature to configure a connection to an online Cloudant service. Specify the URL, `userid`, and password of your existing Cloudant account in the `couchdb` configuration element. For example:

```
<couchdb id='couchdb' jndiName='couchdb/connector' libraryRef='couchdb-lib' url='https://mylink.cloudant.com/' userna

```

See the documentation for “Liberty:The limits to protection through password encryption” on page 1009 to learn about how to secure passwords in configuration files.

## What to do next

Now that you have configured your application to enable the use of CouchDB, you are ready to test the use of CouchDB from your application.

## Planning to use optimized local adapters in Liberty for z/OS



Plan how to implement WebSphere optimized local adapters (WOLA) in your Liberty server environment.

### Before you begin

For CICS Transaction Server for z/OS to communicate with optimized local adapters, the minimum required version of CICS Transaction Server for z/OS is version 4.1.

### About this task

If you have applications that are written in native languages, such as Cobol, PL/I, C/C++, and high-level assembly languages, that run under z/OS batch, Customer Information Control System (CICS), or UNIX System Services environments, you can use optimized local adapters to directly call between the native-language application and Java-based business logic on a Liberty server. You can use optimized local adapters to make the following calls:

- Inbound calls from an external address space to Enterprise JavaBeans (EJB) applications that are deployed on a local Liberty server
- Outbound calls from an application that is running under the Liberty server on z/OS to a server program that is running in an external address space

If you have a large number of native-language applications that you want to use on Liberty, implementing optimized local adapters provides the following benefits:

- Performance improvement
- Identity context propagation
- Local binding support
- Gateway or proxy for legacy assets on z/OS systems

## Procedure

1. Review the existing business and middleware applications in your environment to determine which application processes would benefit from using optimized local adapters. Choose processes that you can remove and replace with calls to the optimized local adapter native API callable services.  
For more information about when to use optimized local adapters, see “Optimized local adapters on Liberty for z/OS” on page 1690 and “Optimized local adapters usage scenarios for Liberty for z/OS” on page 1693.
2. If you plan to propagate a System Authorization Facility (SAF) user ID from Liberty for z/OS to the enterprise information system (EIS), verify that the Liberty server is using a SAF-based user registry. For more information, see “Activating and configuring the SAF registry on z/OS” on page 1857.
3. Review the optimized local adapters samples. There are several examples that are included when you install Liberty for z/OS. For information about using the samples, see “Optimized local adapters samples for Liberty” on page 1691.
4. Decide how to use optimized local adapters. You can use the optimized local adapters to make inbound or outbound calls.
  - a. Use the optimized local adapters to call inbound to Liberty server EJB applications.

The following image shows the flow of an inbound CICS call to a Liberty server EJB application.

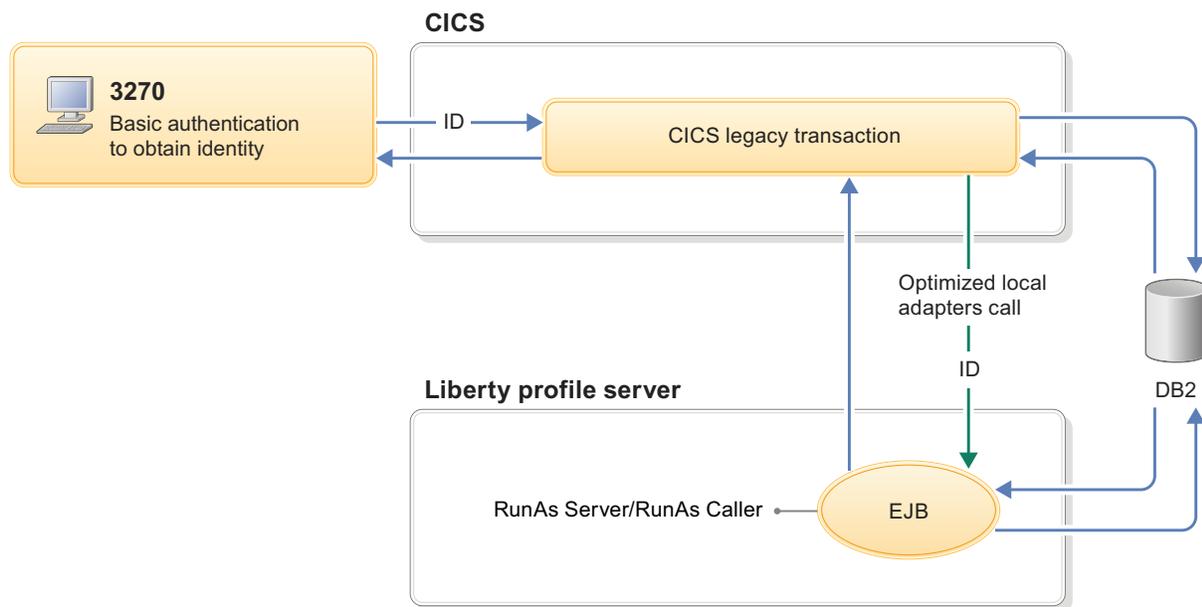
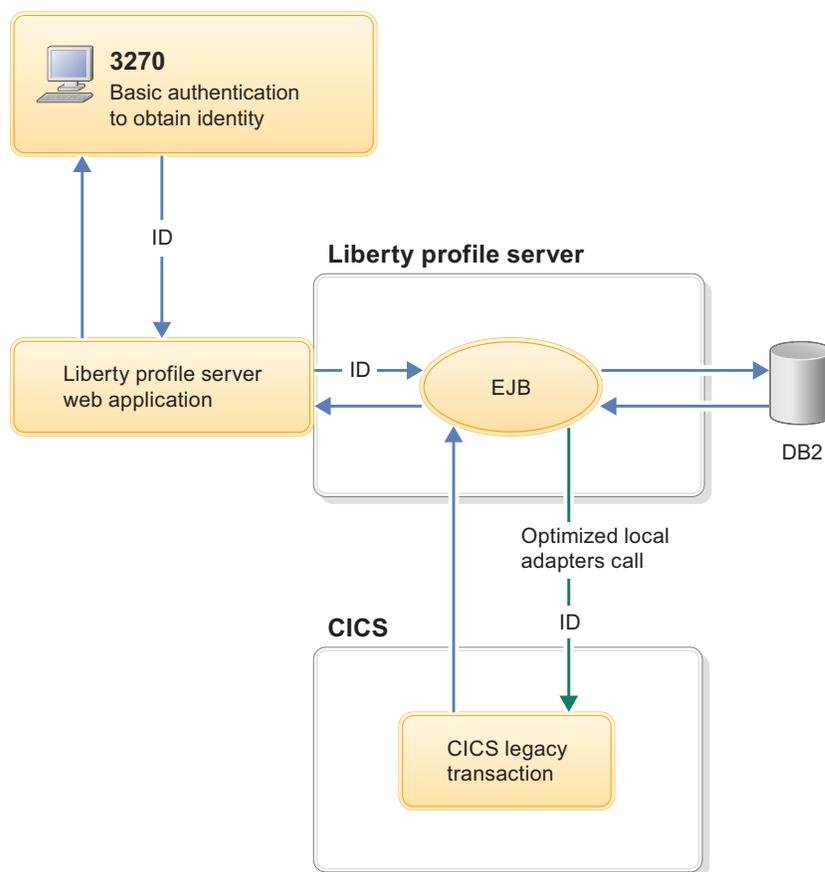


Figure 28. Using CICS

- b. Use the optimized local adapters to call programs in external address spaces from Liberty server applications.

The following figure shows the flow of an outbound Liberty server call to a CICS transaction.



For more information about using optimized local adapters, see “Enabling the Liberty server environment to use optimized local adapters” on page 1697 and “Optimized local adapters APIs on Liberty for z/OS” on page 2079

**Optimized local adapters on Liberty for z/OS:** z/OS 8.5.5.2

Optimized local adapters support on Liberty for z/OS consists of a set of callable services and a Java EE Connector Architecture (JCA) 1.5 resource adapter. The services and adapter work together to provide high-performance calling between native-language applications on z/OS and business logic in a Liberty server environment.

You can use WebSphere optimized local adapters (WOLA) to make inbound calls to applications that are deployed on Liberty from an external address space. You can also use optimized local adapters to make outbound calls from Liberty applications to applications that are running in an external address space on the same z/OS system.

With this support, existing z/OS applications that are written in Cobol, PL/I, C, C++, and assembly language can achieve high performance and efficient integration with Java applications that are deployed on the Liberty server on the same z/OS system.

Optimized local adapters also provide close integration of qualities of service (QoS), including support for fast thread-level security propagation and assertion between the API-exploiting external address spaces and the Liberty server. Support is provided for using the adapters APIs in the following environments:

- Customer Information Control System (CICS)
- UNIX System Services
- Batch processing

A task-related user exit (TRUE) program is provided to support the optimized local adapters under CICS.

## Benefits of using optimized local adapters

### Performance improvement

You can achieve significant performance characteristics when you use the optimized local adapters APIs to call into applications that are deployed on a Liberty server from local batch and UNIX System Services, and CICS applications. The ability to pass parameter data using binary techniques provides a large part of the performance improvement. The transport-level support that the adapters provide uses z/OS cross-memory services to optimize the performance of calls to applications that are deployed on a locally accessible Liberty server.

### Identity context propagation

For inbound requests to the Liberty server using the optimized local adapters APIs, the user ID on the existing z/OS thread is always propagated and asserted in the Liberty EJB container. For calls from CICS, you can extend this propagation by specifying a registration option that propagates and asserts the identity of the CICS task-level user. For calls from Liberty applications, you can propagate and assert identity under CICS using the optimized local adapters CICS link server. You can control this behavior by specifying a flag on the Register API.

### Local binding support

Optimized local adapters can provide a high-performance local binding for existing applications, middleware, and subsystems on z/OS platforms. If there is a local Liberty server available, these local bindings are used with current programming interfaces.

### Gateway or proxy for legacy assets on z/OS systems

Optimized local adapters provide the basis for you to use the Liberty stack as an easily accessible set of capabilities. These capabilities extend the life of application assets that might be difficult to replace. When you use an enterprise bean as a proxy, any Cobol, assembly language, or C/C++ application that is deployed on a z/OS system can easily become a web services client or a Web 2.0 application requester that reaches a set of web applications that are within reach of your locally running application server.

Using the Liberty outbound APIs, any Cobol, assembly language, or C/C++ application can be presented to the Liberty server as a callable service. You can then deploy a provider web services application in the local Liberty server that accepts requests as a gateway for this backend service. In this scenario, the JCA 1.5 programming model sends requests to the application, receives responses from it, and sends back responses to the web-based caller.

## Optimized local adapters samples for Liberty:

z/OS



8.5.5.2

Use the WebSphere optimized local adapters (WOLA) sample files to quickly get started using the optimized local adapters on Liberty.

The sample files for optimized local adapters on Liberty are available on GitHub. For information about how to install the samples, see the readme file on GitHub.

- “Job Control Language (JCL) samples”
- “Program List Table (PLT) samples” on page 1692
- “Link server samples” on page 1692
- “Samples for inbound calls” on page 1692
- “Samples for outbound calls” on page 1693

### Job Control Language (JCL) samples

- CSDUPDAT.jclsamp - The CSDUPDAT program is a Customer Information Control System (CICS) DFHCSDUP utility job that defines all resource definitions that are needed to use optimized local adapters under CICS.

- DFHPLTOL.jclsamp - The DFHPLTOL program contains JCL source code for assembling a sample Program List Table (PLT) with the sample program to enable the task-related user exit (TRUE), BBOACPLT, and the sample BBOC command processor PLT, BBOACPL2.
- OLABATCH.jclsamp - The OLABATCH program contains JCL source code to run one of the samples in z/OS batch. This sample must run on the same logical partition (LPAR) as the Liberty server.

### Program List Table (PLT) samples

- BBOACPLT.cicsasm - The BBOACPLT program contains assembly language sample source code for a CICS PLT initialization routine that shows how to enable the optimized local adapter TRUE during CICS startup.
- BBOACPL2.cicsasm - The BBOACPL2 program contains assembly language sample source code for a CICS PLT initialization routine that shows how to get optimized local adapter INITPARMS from CICS startup parameters and issue the BBOC STRT\_SRVR command during CICS startup.
- BBOACPL3.cicsasm - The BBOACPL3 program contains assembly language sample source for a CICS PLT initialization routine that shows how to pass multiple BBOC commands to the BBOACNTL program during CICS startup.

### Link server samples

- OLACB01.jclsamp - The OLACB01 program contains JCL source code for a CICS program that can be called from the link server. The program uses a COMMAREA object to pass its parameters. Use this sample target program with the optimized local adapter CICS link server. The program echoes back the sent message.
- OLACB02.jclsamp - The OLACB02 program contains JCL source code for a CICS program that can be called from the link server. The program uses a CONTAINER object to pass its parameters. Use this sample target program with the optimized local adapter CICS link server. The program echoes back the sent message.
- OLACB10.jclsamp - The OLACB10 program contains JCL source code for a CICS program that can be called from the link server. The program uses multiple containers to pass data to CICS from an EJB bean. Use this sample target program with the optimized local adapter CICS link server.
- OLACB11.jclsamp - The OLACB11 program contains JCL source code for a CICS program that can be called from the link server. The program uses multiple containers to pass data to CICS from an EJB bean, and modifies that data within the program. Use this sample target program with the optimized local adapter CICS link server. The data is modified inside the target program.
- OLACB12.jclsamp - The OLACB12 program contains JCL source code for a CICS program that can be called from the link server. The program uses multiple containers to pass data to CICS from an EJB bean, and shows how objects can be removed from the request container so that they are not sent in the response container. Use this sample target program with the optimized local adapter CICS link server. The data is deleted inside the target program.

### Samples for inbound calls

- OLACB05.jclsamp - The OLACB05 program contains JCL source code for a CICS sample Cobol program that demonstrates how to use the APIs to register, get a connection, call an EJB bean with the Send Request API, get the response, and release the connection, and unregister.
- OLACB06.jclsamp - The OLACB06 program contains JCL source code for a CICS sample Cobol program that demonstrates how to use the APIs to register, call an EJB bean with the Invoke API, and unregister.
- OLACC01.jclsamp - The OLACC01 program contains JCL source code for a C program that demonstrates how to use the APIs to register, call an EJB with the Invoke API, and unregister. You can run this sample under batch, UNIX System Services, or CICS.

## Samples for outbound calls

- OLACB03.jclsamp - The OLACB03 program contains JCL source code for a CICS sample Cobol program that demonstrates how to make a CICS task into an optimized local adapter server by using the Host Service API.
- OLACB04.jclsamp - The OLACB04 program contains JCL source code for CICS sample Cobol program that demonstrates how to make a CICS task into an optimized local adapter server by using the Receive Request and Get Data APIs.
- OLACC02.jclsamp - The OLACC02 program contains JCL source code for C program that calls the Host Service, Send Request, Send Response, and Get Data APIs. This program essentially invokes itself, calling in to an EJB that then calls back to this program. You can run this sample under batch, UNIX System Services, or CICS.

## Optimized local adapters usage scenarios for Liberty for z/OS:

z/OS



8.5.5.2

Real-world scenarios illustrate how optimized local adapters and the supporting native API callable services provide can benefit enterprise architecture and application development on the z/OS platform.

WebSphere optimized local adapters (WOLA) provide existing native-language business and middleware applications in z/OS batch, Customer Information Control System (CICS), and UNIX System Services environments an alternative way to call Java applications that are implemented as Enterprise JavaBeans (EJB) applications on Liberty. Using optimized local adapters, you can also call from Liberty applications to an external server program that is running locally or on the same logical partition (LPAR) using Java EE Connect Architecture (JCA) Version 1.5.

A scenario where the optimized local adapters can provide increased performance is CICS support for the use of server and client web services. The targeted backend applications can call business logic that is located elsewhere more efficiently when using the optimized local adapters instead of XML and SOAP messaging technology.

The following hypothetical real-world scenarios describe how optimized local adapters are useful to achieve various business goals.

### Financial services company scenario

An IBM z/OS financial services customer that is running business applications under z/OS batch must decide about purchasing a financial processing application, which provides new support for stock trade real-time reporting to the exchanges. The ability to do this style of real-time reporting can result in increasing revenue for the customer.

The application that does real-time reporting is a Java Enterprise Edition (Java EE) application on a Liberty server that runs on Windows 8. The application offers a set of enterprise beans and associated web services interfaces that can be called for various kinds of interactions.

A test scenario is developed and successfully implemented to call the Java EE application from a batch Cobol program. Therefore, the customer decides to move forward and do more rigorous testing. Further testing shows that when this mechanism is pressed by more than 50-100 requests per second, it begins to slow to the point where the response times do not meet the customer requirements. The effort is abandoned until a more realistic approach is available for exchanging information in real time between the batch business application and the new vendor application.

The optimized local adapters can provide this batch customer with an option to deploy Liberty for z/OS and update the batch application to use the optimized local adapters Invoke or Send Request API. These APIs provide a way to call EJB applications that are deployed on a local Liberty server, which calls the business logic for the web service.

## Insurance company scenario

An IBM z/OS insurance industry customer that is running a business application under CICS wants to provide customers with the ability to retrieve and update policy information in real time. This information must be gathered in various ways and from several places, including:

- Information that is directly gathered from DB2
- Information that is gathered by calling a program in CICS
- Information that is gathered by starting a web service to communicate with a remote service provided by another company

The customer chooses to use a Java application for several reasons, but most importantly because most of their programming skills are based in Java. When the new application is tested, the customer experiences long response times when retrieving information. The slow response time is a result of the Liberty server running on a distributed server and the latency that is involved with communicating remotely with DB2 while it calls CICS using web services and SOAP messages.

To fix the problem, the customer deploys multiple Liberty servers in the same configuration to reduce the number of requests per second on any one of the servers and to spread the requests across separate network paths.

Using optimized local adapters gives the customer an alternative other than deploying multiple servers. The customer could install the application on a Liberty server on z/OS, closer to the DB2 and CICS environments. Using the optimized local adapters APIs for the calls to CICS from the Liberty server provides a significant improvement over the web services and SOAP solution. Consolidating on z/OS platforms reduces the need for more distributed servers that consume floor space, power, and resources to maintain. In this scenario, because the location of the data and applications is the gating factor, increasing the size of the remote server to the most robust one available does not necessarily solve the problem.

## Migrating business logic to Liberty for z/OS

A customer has years of application logic with Cobol running inside of CICS. They want to migrate some of these applications to Liberty to take advantage of Java and Java EE technologies and use other capabilities in the WebSphere stack.

One of the applications is too large to migrate in one piece, and they want to gradually move portions of it to a Liberty server. The transactional and security qualities of service that CICS provides must be maintained during the migration, and the performance impact of the migration must be minimal. Using optimized local adapters, portions of the application can be migrated to Liberty and wrapped in a stateless session bean. The Cobol application logic can be modified to use the optimized local adapter to call the stateless session beans. These calls to the Liberty server run under the same transaction and security contexts that are used by the Cobol programs in the CICS region. There is a significant performance gain when compared to making similar calls using a web service. The customer can continue to relocate portions of the application to the Liberty server until the application is migrated.

## Optimized local adapters performance considerations for Liberty: 8.5.5.2

The WebSphere optimized local adapter (WOLA) APIs are designed to provide optimal performance for calling between an external address space and applications on Liberty for z/OS. The APIs establish new kinds of application patterns by supporting fine-grained interactions between applications in these environments. By choosing the best configuration options for your system, you can maximize the performance benefits of using the optimized local adapters.

## Selecting minimum and maximum connection values for the Register API call

Selecting a minimum connections value for the Register API call that is too large can degrade performance. Because each established connection remains until the Unregister API is called, a minimum connection value that is too large consumes more memory and increases the time that is needed to complete each Register and Unregister API call. Select the smallest minimum connections value that suits your needs; for example, if hundreds of simultaneous threads can potentially share a registration, then it might make sense to dedicate more memory and time to registration with a large minimum connections value. If you expect fewer concurrent threads, set a smaller minimum connections value.

Selecting a value that is too small for the maximum number of connections can also degrade performance if the client must wait for a connection when it requests one. When the maximum connections value is exceeded, the calling thread waits the number of seconds specified on the wait time parameter for Connection Get, Invoke, Receive Request Any, or Host Service APIs for a connection to become available. When this time expires, return and reason codes are passed back that indicate that a connection handle could not be acquired for the request before the wait time expired. Select a maximum connections value that best fits the anticipated needs of your environment.

## Selecting maximum connection values when you start a CICS link server

When you start a link server task under Customer Information Control System (CICS) without specifying the minimum connections (MNC) and maximum connections (MXC) parameters, MNC defaults to 1 and MXC defaults to 10. The value of the MXC parameter specifies the number of link invocation tasks (BBO#) that can be started and concurrently run by the link server task (BBO\$). As a result, the value also limits the number of concurrent threads on the Liberty server that can run and start CICS target programs.

Select an MXC value that reflects the expected duration of the typical target CICS programs that are started under this instance of the link server. For example, if the target CICS programs are mostly long-running, a larger MXC value is appropriate to keep requests flowing efficiently from the Liberty server into CICS. If the target programs are short-lived, a smaller MXC value is more efficient.

## Shared 64-bit memory

When the optimized local adapters feature is enabled in a Liberty server, the server obtains 32 MB of shared memory that is located above the 2 GB bar in z/OS. This memory is shared by all Liberty servers with the same wolaGroup name and stores the shared optimized local adapter control structures.

Additional shared memory that is located above the 2 GB bar is allocated to store messages passed between a client and a Liberty server. The amount of storage that is required to pass messages depends on the average size of the messages that are passed, and there must be enough shared memory to hold all of the message data that exists at any one time. Additional memory is allocated as required.

If an application continues to call the Register API and loop without calling the Unregister API and without terminating, which automatically cleans up these registrations, it can overflow the optimized local adapters shared memory buffer for the WOLA group. If this occurs, API calls are returned with out-of-memory reason codes.

You can calculate a rough estimate of the amount of WOLA shared memory that your application needs. Each client registration consumes 384 bytes of shared memory plus 192 bytes of shared memory for each connection. A registration with a maximum of 100 connections consumes about 20 KB of shared memory. Each client thread, which must wait for a connection to become available if all connections are in use, consumes an additional 80 bytes. Each service that the registration hosts consumes an additional 384 bytes.

For example, suppose you have 200 registrations in your WOLA group. Each registration contains 200 connections, and has a maximum of 1,000 threads waiting for a connection at any time. The total memory consumed by this configuration is about 24 MB, which leaves enough shared memory to host about 25,500 services concurrently or 125 concurrent services per registration.

200 Registrations x 384 bytes =	76,800 bytes
200 Registrations x 200 connections x 192 bytes =	7,680,000 bytes
200 Registrations x 1000 waiters x 80 bytes =	16,000,000 bytes
-----	
	23,756,800 bytes
33,554,432 bytes - 23,756,800 bytes =	9,797,632 bytes remaining
	/ 384 bytes per service
-----	
	25,514 services

### Optimized local adapters CICS link server performance considerations

You can use optimized local adapters for a CICS link server as a simple way to invoke existing CICS application programs from applications that are running on the Liberty server. When you start the link server, the optimized local adapters link server task (BBO\$) starts and receives program link requests from the Liberty server. When a link request is received, the link server task (BBO\$) initiates the program link task (BBO#), which in turn issues an EXEC CICS LINK command to the target program, receives a response, and sends it to the Liberty server caller. To perform these actions, the thread-level identity of the application on the Liberty server is propagated and asserted onto the target CICS task by setting the SEC=Y parameter on the BBOC **START\_SRVR** command.

You can improve performance by running a link server with SEC=N and using the identity of the user ID that initiated the link server, but this approach might not meet the security and auditing requirements of your organization. If you decide to run the link server with SEC=N, you can further improve performance by also specifying REU=Y on the BBOC **START\_SRVR** command. When you set REU=Y, the link server reuses the program link invocation tasks (BBO#) between program invocation requests.

**Important:** If you run the link server with SEC=N and REU=Y, the optimized local adapter JCA no longer supports passing a separate link transaction ID. Requests for a separate transaction ID result in a ResourceException in the application. If you attempt to run the link server with SEC=Y and REU=Y, the reuse option is forced to No because the link server must start a new program link task for each request and assert the propagated identity.

If you run a link server with REU=Y, program link tasks (BBO#) remain active until a BBOC **STOP\_SRVR** or **UNREGISTER** command is entered for the registration. If you are also running with a high maximum connections (MXC) value and a large number of requests arrive concurrently, the number of active program link tasks (BBO#) might reach the CICS maximum concurrent task threshold. For more information about setting the CICS maximum concurrent task threshold, see the documentation for your version of CICS.

To achieve the fastest performance when you call into an application under CICS from the Liberty server, code the Host Service, Receive Request Any, or Receive Request Specific APIs directly in your application program. However, coding the APIs directly does not provide the built-in support for identity propagation that the link server provides.

### Considerations for using the JCA resource adapter

When you use the optimized local adapter JCA resource adapter, each connection that is obtained from the ConnectionFactory object requires additional memory overhead. If your application makes several

calls to an external address space or CICS in the same application method, you can achieve better performance by using the same connection for each interaction and using the same JCA interaction object within an application method.

When you create the JCA ConnectionFactory object for optimized local adapters, you can modify the minimum and maximum size of the JCA connection pool for that ConnectionFactory. The connection pool represents logical connections that are bound to physical connections that are specified when you call the Register API during an interaction. For optimal performance, set the size of the JCA connection pool to be the same size of the physical connection pool that you set during the Register API call. If your JCA connection pool is too small, your application might have to wait for a JCA connection object, even though there are physical connections available.

## Administering optimized local adapters on Liberty for z/OS



Enable optimized local adapters and register an external address space with a local Liberty server.

### Enabling the Liberty server environment to use optimized local adapters:

You must enable the Liberty server to receive inbound and outbound requests using the optimized local adapters support. WebSphere optimized local adapters (WOLA) for z/OS are a set of callable services (APIs) that give native z/OS applications the ability to make inbound calls to application server enterprise beans and enable native programs to act as a server and accept requests from applications running in the WebSphere Liberty server.

#### Before you begin

 Use IBM Installation Manager to install Liberty for WebSphere Application Server Version 8.5.5.2, along with the following interim fixes:

- 8.5.5.2-WS-WLP-OS390-IFPI18279
- 8.5.5.2-WS-WLP-OS390-IFPI18379

Download the interim fixes from IBM Fix Central, or install the interim fixes directly from the service repository. After you install the interim fixes, use the featureManager command to install the zosLocalAdapters-1.0 feature in your Liberty environment. For more information, see “Installing assets using the featureManager command” on page 1403.

 Use IBM Installation Manager to install Liberty for WebSphere Application Server Version 8.5.5.3 or later. Install the zosLocalAdapters-1.0 feature in your Liberty environment. For more information, see “Installing Liberty Repository assets” on page 1391.

#### Procedure

1. Allocate or select a load module library to contain the optimized local adapter load modules. This library is used by applications that are running outside the Liberty server. The library must be a PDS-E and requires approximately 40 tracks (3390) to hold the optimized local adapter modules.
2. Copy the optimized local adapter load modules from wlp/clients/zos/\* to the load module library. The following example shows how to copy load modules into the \$DSNAME data set:  

```
cp -Xv wlp/clients/zos/* "'/'$DSNAME'"
```
3. To enable optimized local adapters support on the Liberty server, configure the zosLocalAdapters-1.0 feature in the server.xml file.
  - a. To enable the feature, add the zosLocalAdapters-1.0 feature to the server.xml file as shown in the following example.

```
<featureManager>
  <feature>zosLocalAdapters-1.0</feature>
</featureManager>
```

- b. Create a WOLA group by configuring a `zosLocalAdapters` element with a three-part WOLA group name in the `server.xml` file. The three-part WOLA group name is used by clients to connect to the Liberty server. Each part of the group name must be 1 to 8 alphanumeric characters.

**Note:** Do not use lowercase characters in the WOLA group name. The z/OS security subsystem converts lowercase characters to uppercase, which can cause a mismatch with your configuration.

```
<zosLocalAdapters wolaGroup="LIB1" wolaName2="LIB2" wolaName3="LIB3"/>
```

4. Configure a connection factory by adding a `connectionFactory` element to the `server.xml` file and specifying its properties in a `properties.ola` element.

```
<connectionFactory jndiName="eis/ola">
  <properties.ola RegisterName="OLASERVER"/>
</connectionFactory>
```

For information about WOLA connection factory properties, see “Connection factory properties for optimized local adapters on Liberty” on page 1699.

5. Create SERVER profiles for z/OS.
  - a. Create SERVER profiles for the optimized local adapter authorized service. Use the following Time Sharing Option (TSO) commands:

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.LOCALCOM UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.LOCALCOM CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.WOLA UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.WOLA CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

- b. Create a SERVER profile for the authorized client module BBGZSCFM and permit the Started Task user ID of the Liberty server to the profile. This action enables a Liberty server to load the z/OS Authorized client services. To enable a server that is running as WLPUSER1 to access the authorized client module:

```
RDEF SERVER BBG.AUTHMOD.BBGZSCFM UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSCFM CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

- c. Create SERVER profiles for optimized local adapter authorized client service. Use the following TSO commands:

```
RDEF SERVER BBG.AUTHMOD.BBGZSCFM.WOLA UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSCFM.WOLA CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

For more information, see “Enabling z/OS authorized services in Liberty for z/OS” on page 1942.

6. If you have CBIND enabled in System Authorization Facility (SAF), grant access to the clients that will use optimized local adapters.

- a. Define a profile for the Liberty server in the CBIND class. The profile name is `BBG.WOLA.<WOLA1>.<WOLA2>.<WOLA3>`, where `WOLA1`, `WOLA2`, and `WOLA3` are the three parts of the optimized adapter group name that are specified in the `<zosLocalAdapters>` element in the `server.xml` file. You can define a profile by using the SAF **RDEFINE** TSO command. For example, the following command creates a profile in the CBIND class for a WOLA group named `LIB1.LIB2.LIB3`:

```
RDEF CBIND BBG.WOLA.LIB1.LIB2.LIB3 UACC(NONE)
```

- b. Permit READ access to the profile. For example, the following command permits read access for the `username` user name on the `bbg.wola.lib1.lib2.lib3` profile:

```
PERMIT BBG.WOLA.LIB1.LIB2.LIB3 CLASS(CBIND) ACCESS(READ) ID(USERNAME)
```

You can use asterisks to permit a user access to multiple profiles. The following example permits READ access to the `username` user for all profiles that start with `bbg.wola` in the CBIND class:

```
RDEF CBIND BBG.WOLA.* UACC(NONE)
PERMIT BBG.WOLA.* CLASS(CBIND) ACCESS(READ) ID(USERNAME)
```

For more information about SAF commands and syntax, see the documentation for your version of z/OS.

## Results

You can now deploy and start applications that use optimized local adapters on the Liberty server.

## What to do next

Ensure that all external connections that use the optimized local adapters are running the latest version of the optimized local adapters load module library.

1. Ensure that the load module library is at the latest level.
2. Ensure that the library is made available to all of the external address spaces that use the optimized local adapters. For example, make sure the library is available in the STEPLIB for batch jobs, or in the DFHRPL concatenation for Customer Information Control System (CICS).

If you want to use the optimized local adapters with CICS, you must enable support for the adapters in CICS. For more information, see “Enabling support for Liberty optimized local adapters in CICS” on page 1703.

If you want to create a connection, begin by registering the external address space to the Liberty server. For more information, see “Registering an external address space with a local Liberty server using optimized local adapters” on page 1711.

Connection factory properties for optimized local adapters on Liberty:

z/OS



8.5.5.2

Use the properties for the WebSphere optimized local adapters (WOLA) to configure a connection factory when you enable WOLA on your Liberty server.

One or more connection factories must be configured to enable the optimized local adapters on z/OS for inbound and outbound support, even though the connection factory is only used directly for outbound. For information about configuring a connection factory, see “Enabling the Liberty server environment to use optimized local adapters” on page 1697.

Property	Values	Description
RegisterName	Any alphanumeric string of 1 to 12 characters	This property defines the WOLA register name to use for connections that are obtained from this connection factory.
Username	String; further restrictions on supported values depend on the associated user registry	This property defines a user ID that overrides the user ID that is sent from the connection factory. The <b>Username</b> property is used together with the <b>Password</b> property to authenticate the user and obtain the corresponding MVS user ID.
Password	Any string	This property defines the password that is used together with the <b>Username</b> property to authenticate the user.

Property	Values	Description
LinkTaskTranID	Any 4-character string	When you are using a Customer Information Control System (CICS) link server, this property defines the name of the CICS transaction that starts the link task that processes requests that are issued from the connection factory. This property overrides the link task transaction ID specified by the control transaction (BBOC) when the CICS link server was started.
UseCICSContainer	true, false	When you are using a CICS link server, this property defines whether the input and output messages are passed to the target CICS program in a COMMAREA object or in a CONTAINER object. If this property is set to true, the messages are passed in a CONTAINER object. If this property is set to false, the messages are passed in a COMMAREA object. <b>Note:</b> If the input and output messages are specified using a javax.resource.cci.MappedRecord interface, the messages are always passed in a CONTAINER object.
LinkTaskReqContID	A string of 1 to 16 characters that matches the container name defined to CICS	When you are using a CICS link server, this property defines the name of the CONTAINER object that contains input messages sent to the CICS program. <b>Note:</b> To use this property, the <b>UseCICSContainer</b> property must be set to true.
LinkTaskReqContType	0, 1	When you are using a CICS link server, this property defines whether the input CONTAINER object is defined as a CHAR or a BIT container. If this property is set to 0, the target program expects a CHAR container. If this property is set to 1, the target program expects a BIT container. When a CHAR container is requested, the input data is assumed to be in the ASCII code page, and the data is converted to EBCDIC when the container is created.
LinkTaskRspContID	A string of 1 to 16 characters that matches the container name defined to CICS	When you are using a CICS link server, this property defines the name of the CONTAINER that contains the output message from the CICS program. <b>Note:</b> To use this property, the <b>UseCICSContainer</b> property must be set to true.

Property	Values	Description
LinkTaskRspContType	0, 1	When you are using a CICS link server, this property defines whether the output CONTAINER is defined as a CHAR or a BIT container. If this property is set to 0, the target program sends a CHAR CONTAINER. If this property is set to 1, the target program sends a BIT CONTAINER. When a CHAR CONTAINER is requested, the data from the CICS program is assumed to be in the EBCDIC code page, and the data is converted to ASCII when data is retrieved from the CONTAINER.
LinkTaskChanID	A string of 1 to 16 characters that matches the channel name defined to CICS	When you are using a CICS link server, this property defines the name of the CHANNEL that contains the input and output CONTAINER objects. <b>Note:</b> To use this property, the <b>UseCICSContainer</b> property must be set to true.
LinkTaskChanType	0, 1	When you are using a CICS link server, this property defines whether the input and output CONTAINER objects are defined as CHAR or BIT containers. If this property is set to 0, the target program sends and receives CHAR containers. If this property is set to 1, the target program sends and receives BIT containers. When a CHAR container is requested, the input data is assumed to be in the ASCII code page, and the data is converted to EBCDIC when the containers are created. Similarly, the data from the CICS program is assumed to be in the EBCDIC code page, and the data is converted to ASCII when data is retrieved from the containers. <b>Note:</b> Use this property only when the input and output messages are specified using a <code>javax.resource.cci.MappedRecord</code> interface.

Property	Values	Description
ConnectionWaitTimeout	Any integer between 0 and 2147483647	<p>This property defines the maximum number of seconds that a request waits for a service name to become available. The service name is specified on Interaction objects in connections that are obtained from the connection factory. If the service name is not available after the specified number of seconds elapse, a <code>javax.resource.ResourceException</code> is thrown.</p> <p>Setting this property to 0 disables the timer. The default value for this property is 30.</p>
OTMAGroupID	String of 1 to 8 characters that matches the IMS XCF group name that is defined to IMS.	When you use IBM Information Management System (IMS), this property defines the group name that the IMS region uses to connect to the cross-system coupling facility (XCF). The value should match what is declared in the <code>IMSPBxxx PROCLIB</code> member for the parameter named <code>GRNAME</code> .
OTMAServerName	String of 1 to 16 characters that matches the IMS XCF system name that is defined to IMS.	When you use IBM Information Management System (IMS), this property defines the system name that the IMS region uses to connect to the cross-system coupling facility (XCF). The value should match what is declared in the <code>IMSPBxxx PROCLIB</code> member for the parameter named <code>OTMANM</code> .
OTMAClientName	String of 1 to 16 characters, alphanumeric including national characters, defaulting to the string <code>DEFAULT</code> .	When you use IBM Information Management System (IMS), this property defines the system name that the Liberty server uses to connect to the cross-system coupling facility (XCF). The value should be unique within the XCF group that is used by the IMS region that you connect to.
OTMASyncLevel	0,1	When you use IBM Information Management System (IMS), this property controls the sync level that is used to send messages to and from IMS. A value of 0 uses sync level <code>NONE</code> , and a value of 1 uses sync level <code>CONFIRM</code> .
OTMAMaxSegments	Any integer between 0 and 2147483647	When you use IBM Information Management System (IMS), this property controls the maximum number of segments that a reply message is allowed to contain. The default value is 1.

Property	Values	Description
OTMAMaxRecvSize	Any integer between 0 and 2147483647	When you use IBM Information Management System (IMS), this property controls the maximum number of bytes that a reply message is allowed to contain. The default value is 32768.
OTMARRequestLLZZ	0,1	When you use IBM Information Management System (IMS), this property controls the format of the request message that is sent to IMS. A value of 1, the default, indicates that the request starts with an LLZZ format header. A value of 0 indicates that the request starts with an LLLLZZ header.
OTMARResponseLLZZ	0,1	When you use IBM Information Management System (IMS), this property controls the format of the response message that is received from IMS. A value of 1 indicates that the response starts with an LLZZ format header. A value of 0, the default, indicates that the request starts with an LLLLZZ header.

## Enabling support for Liberty optimized local adapters in CICS:

You must enable your Customer Information Control System (CICS) environment to receive inbound and outbound requests using WebSphere optimized local adapters (WOLA).

### Before you begin

Enable your Liberty server environment to use optimized local adapters. For more information, see “Enabling the Liberty server environment to use optimized local adapters” on page 1697.

### Procedure

1. Add the CICS resource definitions for the optimized local adapters to the primary CICS system definition (CSD) file, DFHCSD. You can either manually add the definitions in CICS or download and run the CSUPDAT sample.
  - In CICS, use the CEDA transaction or an equivalent transaction to add the definitions to the DFHCSD. See “Optimized local adapter definitions for CICS” on page 1705 for the required definitions.
  - Use the CICS offline CSD update program, DFHCSDUP, to add the definitions to the DFHCSD. For more information about the DFHCSDUP program, see the documentation for your version of CICS. See “Optimized local adapter definitions for CICS” on page 1705 for the required definitions.
  - Update the definitions by running the CSDUPDAT.jc1samp sample job.
    - a. Download the optimized local adapter samples. For more information about downloading and installing the samples, see “Optimized local adapters samples for Liberty” on page 1691.
    - b. Copy the samples and CSDUPDAT member to a data set.
    - c. Customize the CSDUPDAT.jc1samp sample job for your environment. For example, in the sample job, enter the name of the dataset where the CSD is located.
    - d. Run the CSDUPDAT.jc1samp sample job.

- Copy the load modules and DLLs that are required for CICS from the Liberty server hierarchical file system (HFS) or zSeries file system (zFS) to a partitioned data set for use under CICS. The following example shows how to copy load modules into the \$DSNAME data set:

```
cp -Xv wlp/clients/zos/* "'/$DSNAME'"
```

- Place the data set in the CICS DFHRPL concatenation.
- Set up the Liberty message catalog in the CICS region. The optimized local adapters programs issue messages from a message catalog that ships with Liberty. For the programs to issue messages, the NLSPATH environment variable in the CICS region must point to the directory that contains the message catalog. This directory is wlp/lib/native/zos/s390x/nls/%N.cat, where wlp is the directory in which the Liberty server is installed.

To set the environment variable, use the Language Environment ENVAR option, which you can set by editing the CEEROPT CSECT that the CICS region uses. After you edit the CSECT, you can build, compile, link, and copy the CSECT into the DFHRPL data set. For more information about other ways to set Language Environment options, see the documentation for your version of CICS.

**Note:** Ways of setting Language Environment options that involve editing the application source code or relinking the application are not supported because the optimized local adapter programs cannot be recompiled or relinked.

The following example shows a CEEROPT CSECT that defines the NLSPATH environment variable for a Liberty server that is installed in /u/MSTONE1/wlp. Note that the definition spans two lines and includes a continuation character, X, in column 72.

```
CEEROPT CSECT
CEEROPT AMODE ANY
CEEROPT RMODE ANY
*****
*
* Utility: CEEROPT
* Purpose: Set default LE runtime options for CICS region.
*
*****
      CEEXOPT ENVAR=(('NLSPATH=/u/MSTONE1/wlp/lib/native/zos/s390x/nlX
                    s/%N.cat'),OVR)
      END
```

- Secure your optimized local adapter connections by performing the following actions:
  - Create SERVER profiles for z/OS.
  - If you have CBIND enabled in System Authorization Facility (SAF), grant access to the clients that will use optimized local adapters.

For more information, see “Securing optimized local adapters for inbound support in Liberty for z/OS” on page 1949.

- Start the optimized local adapters task-related user exit (TRUE) program.

You can start the TRUE program with BBOC, an optimized local adapters transaction for CICS. You can use this transaction to start, stop, enable, and disable tracing for the TRUE module. The TRUE program name is BBOATRUE, which you activate using the BBOC transaction with the START\_TRUE parameter.

When CICS security is enabled, the user ID where the BBOC START\_TRUE and STOP\_TRUE parameters run must have authority to issue the EXEC CICS ENABLE PROGRAM(BBOATRUE) and DISABLE PROGRAM(BBOATRUE) EXITALL commands. Messages that are issued by the Liberty server under CICS are routed to the BBOQ extra partition transient data queue (TDQ) that is allocated under DD BBOOUT in the CICS region.

For more information, see “Liberty server transactions for CICS: BBOC, BBO\$, and BBO#” on page 1705.

- Optional: If you want to use the CICS link server, start the optimized local adapters CICS link server task by issuing the BBOC\_START\_SRVR command on a CICS workstation. For more information, see “Liberty server transactions for CICS: BBOC, BBO\$, and BBO#” on page 1705.

## What to do next

If you want to create a connection, begin by registering the external address space to the Liberty server. For more information, see “Registering an external address space with a local Liberty server using optimized local adapters” on page 1711.

Optimized local adapter definitions for CICS:

z/OS



8.5.5.2

You must define the WebSphere optimized local adapter (WOLA) transactions, programs, task-related user exits (TRUE), and transient data queues (TDQs) in CICS to enable WOLA support.

You must add the definitions that enable WOLA support in CICS to the primary CICS system definition (CSD) file, DFHCSD. For information about how to add the definitions, see “Enabling support for Liberty optimized local adapters in CICS” on page 1703.

When you add the definitions, you can specify the suggested GROUP name, BBOACSD, or you can specify a different name. You must specify all other values as shown in the following example.

```
DEFINE PROGRAM(BBOACNTL) GROUP(BBOACSD) LANGUAGE(C)
    DATALOCATION(ANY) EXECKEY(CICS)
    CONCURRENCY(THREADSAFE) API(OPENAPI)
DEFINE PROGRAM(BBOATRUE) GROUP(BBOACSD) LANGUAGE(ASSEMBLER)
    DATALOCATION(ANY) EXECKEY(CICS)
    CONCURRENCY(THREADSAFE) API(OPENAPI)
DEFINE PROGRAM(BBOACSRV) GROUP(BBOACSD) LANGUAGE(C)
    DATALOCATION(ANY) EXECKEY(CICS)
    CONCURRENCY(THREADSAFE) API(OPENAPI)
DEFINE PROGRAM(BBOACLNK) GROUP(BBOACSD) LANGUAGE(C)
    DATALOCATION(ANY) EXECKEY(USER)
    CONCURRENCY(THREADSAFE) API(OPENAPI)
DEFINE TRANSACTION(BBOC) PROGRAM(BBOACNTL) GROUP(BBOACSD)
    TASKDATALOC(ANY) TASKDATAKEY(CICS)
DEFINE TRANSACTION(BBO$) PROGRAM(BBOACSRV) GROUP(BBOACSD)
    TASKDATALOC(ANY) TASKDATAKEY(CICS)
DEFINE TRANSACTION(BBO#) PROGRAM(BBOACLNK) GROUP(BBOACSD)
    TASKDATALOC(ANY) TASKDATAKEY(USER)
DEFINE TDQUEUE(BBOQ) TYPE(EXTRA) DDNAME(BBOOUT) GROUP(BBOACSD)
    DATABUFFERS(1) BLOCKFORMAT(UNBLOCKED) RECORDF(V)
    TYPEFILE(OUTPUT) DISPOSITION(SHR) OPENTIME(INITIAL)
    BLOCKSIZE(224) RECORDSIZE(220)
```

Liberty server transactions for CICS: BBOC, BBO\$, and BBO#:

z/OS



8.5.5.2

WebSphere optimized local adapters (WOLA) are supported in the CICS product through the BBOC, BBO\$, and BBO# transactions.

The optimized local adapters run in a CICS region as a *resource manager*. In CICS, the Task Related User Exit (TRUE) is the primary vehicle that is used by resource providers. TRUE support provides the boundary between the CICS application threads and the external resource manager threads. Currently, DB2, WebSphere MQ, and TCPIP sockets run in CICS using the TRUE support.

Applications that run under CICS use the optimized local adapter APIs according to the following workflow:

1. The application runs the provided stub routines.
2. The stub routines start the CICS resource manager interface module, passing it the name of the optimized local adapter TRUE routine, BBOATRUE, and the parameters specific to each API.
3. CICS dispatches the TRUE on one of the OPENAPI task control blocks (TCBs) and runs until the API call is completed.
4. The call goes back to CICS with the output parameters.

See the following sections for more information about the Liberty server transactions for CICS:

- “Control transaction for CICS: BBOC”
  - “Sample BBOC commands” on page 1709
  - “Automatically running a BBOC command during CICS startup” on page 1710
- “Link server transaction for CICS: BBO\$” on page 1711
- “Program link invocation transaction for CICS: BBO#” on page 1711

### Control transaction for CICS: BBOC

The BBOC transaction is the WebSphere control, or operations transaction, for the adapters support under CICS. You can use the transaction to enable and start the Liberty server TRUE and to set tracing levels for debugging the APIs and code that interfaces with the Liberty server. BBOC also sets registrations and unregistrations, and starts and stops link server tasks in CICS. These server tasks provide support for starting existing CICS programs and passing data with COMMAREA objects or containers with the input parameters over the adapters. BBOC is a CICS workstation-based transaction that you can run on a 3270 workstation or from a sequential, or SDSCI-type, workstation.

The syntax for the BBOC transaction is BBOC operation\_name **parameters**, where multiple parameters are separated by one or more spaces.

#### RGN

The 12-character register name

#### DGN

The first eight-character name of the WOLA group to join

#### NDN

The second eight-character name of the WOLA group to join

#### SVN

The third eight-character name of the WOLA group to join

#### LSYNC

LSYNC controls whether CICS passes the SYNCONRETURN option when it links to the target program. If you specify LSYNC=Y, the CICS link server passes the SYNCONRETURN option on the EXEC CICS LINK command. You might need to specify this option when the target program is in another CICS region. The default value is LSYNC=N.

#### SVC

The service name of a maximum of 8 characters. The parameter supports masking with asterisks (\*); for example, you can specify \*, abc\*, \*abc, abc\*xyz, abc\*xy\*z, and so on.

#### MNC

The number of minimum connections. The minimum value is 0, and the default value is 1.

#### MXC

The maximum number of connections. The maximum value is 9999, and the default value is 10.

#### SEC

The SEC parameter controls which user ID is propagated. The default value is SEC=N.

If you specify SEC=N and are calling from CICS to the Liberty server, the CICS region user ID is propagated. If you specify SEC=N and are calling from the Liberty server to CICS under the link server task (BBO\$), the link task runs under the user ID of the started link server.

If you specify SEC=Y and are calling from CICS to the Liberty server, the task-level user ID is propagated to the Liberty server. If you specify SEC=Y and are calling from the Liberty server to CICS, the link server attempts to start the link task (BBO#) with the propagated user ID from the Liberty

server. The propagation works only if you created a System Authorization Facility (SAF) SURROGAT class definition to permit the user ID of the link server to issue the EXEC CICS START TRAN('BBO#') USERID(<propagated\_id>) command.

#### STX

The four-character name of the link server CICS transaction ID to use. The default value is BBO\$.

**Note:** If you define a transaction name that is different from the default, you must also define the transaction in the primary CICS system definition (CSD) file, DFHCSD, with the same program name and attributes as BBO\$.

#### LTX

The four-character name of the link-to-program CICS transaction ID to use. The default value is BBO#.

**Note:** If you define a transaction name that is different from the default, you must also define the transaction in the primary CICS system definition (CSD) file, DFHCSD, with the same program name and attributes as BBO#.

#### TRC

Defining a value for this parameter enables tracing at the following levels:

- When set to 0: No tracing; error messages only
- When set to 1: Basic tracing
- When set to 2: Detailed tracing

#### TDQ

The four-character name of the CICS extra-partition transient data queue (TDQ) where adapter messages are written. If you do not specify this parameter, the default is BBOQ and DD BBOOUT. If messages cannot be written to the specified TDQ, they are written to the CICS region stdout, tdq CESO dd CEEOUT.

#### REU

REU controls whether the link server reuses the program link invocation tasks (BBO# transactions) between program invocation requests. The default value is N.

**Important:** If you run the link server with SEC=N and REU=Y, the optimized local adapter JCA no longer supports passing a separate link transaction ID. Requests for a separate transaction ID result in a ResourceException in the application. If you attempt to run the link server with SEC=Y and REU=Y, the reuse option is forced to No because the link server must start a new program link task for each request and assert the propagated identity.

#### REUC

The number of requests for which the CICS link task (BBO#) remains active and is reused. When this count is reached, the link task ends. The maximum value is 2147483648.

**Important:** For a transactional scenario, the link task ends after the count is reached and the next commit is received from the Liberty server.

#### REUT

The number of seconds that the CICS Link task (BBO#) remains active and is reused. When this time interval expires, after the next request is received and processed, the link task ends. The maximum value is 2147483648.

**Important:** For a transactional scenario, the link task ends after the requested time is reached and the next commit is received from the Liberty server.

#### 0.5.5.2 TXN

TXN describes the transactional behavior of the registration that is generated by the BBOC transaction. This option is only supported by registrations to WebSphere Traditional server instances.

When BBOC creates a WOLA registration by using the REGISTER operation, TXN=Y signifies that any Java Platform, Enterprise Edition applications started in the WebSphere Application Server that use this registration joins the current CICS unit of work. When TXN=Y, a global transaction is created between CICS and WebSphere Application Server, which completes by using the two-phase commit protocol when the CICS application issues an EXEC CICS SYNCPOINT, or when a sync point is implied, such as when the CICS task ends.

When BBOC is used to create a link server by using the START\_SRVR function, TXN=Y signifies that the CICS link server task joins the current WebSphere Application Server transaction when a service is started. For example, if a Java Platform, Enterprise Edition application starts a resource manager local transaction (RMLT) and starts a CICS program by using the optimized local adapters JCA connector, the link task joins the local transaction and then starts the target CICS program. Updates that are made in the CICS program are not committed or backed out until the Java Platform, Enterprise Edition application completes the RMLT by using the commit or rollback API.

**Table 122. BBOC.** The following table summarizes BBOC operation names, descriptions, and parameters.

Operation name	Abbreviation	Description	Parameters
START_TRUE	STR	Start the Liberty server TRUE	TRC=<0 1 2> TDQ=<tdqname>
STOP_TRUE	PTR	Stop the Liberty server TRUE	TRC=<0 1 2> TDQ=<tdqname>
REGISTER	REG	Register with the Liberty server WOLA group	RGN=<name> DGN=<name> NDN=<name> SVN=<name> MNC=<minimum_number_of_connections> MXC=<maximum_number_of_connections> SEC=<Y N> TRC=<0 1 2> TDQ=<tdqname> TXN=<Y N>
UNREGISTER		Unregister with the Liberty server optimized local adapters	RGN=<name>

Table 122. BBOC (continued). The following table summarizes BBOC operation names, descriptions, and parameters.

Operation name	Abbreviation	Description	Parameters
START_SRVR	STA	Start the Liberty server task for the passed register name.	RGN=<name> DGN=<name> NDN=<name> SVC=<name> SVN=<name> MNC=<minimum_number_of_connections> MXC=<maximum_number_of_connections> SEC=<Y N> STX=<CICS_link_server_transaction_ID> LTX=<CICS_link_server_transaction_ID> TRC=<0 1 2> TDQ=<tdqname> REU=<Y N> REUC=<number_of_requests> REUT=<number_of_seconds> TXN=<Y N>
STOP_SRVR	STP	Stop the Liberty server task for the register name.	RGN=<name> TRC=<0 1 2> TDQ=<tdqname>

### Sample BBOC commands

The following are samples of BBOC invocations that demonstrate how various tasks and configurations can be accomplished with the CICS adapters program link support.

- Start the adapters CICS TRUE program.  
`bboc start_true`
- Stop the adapters CICS TRUE program.  
`bboc stop_true`
- Register with the name, CICS-HR1, in the WOLA group with names LIB1, LIB2, and LIB3, with 10 maximum connections, 5 minimum connections, and security propagation.  
`bboc register rgn=CICS-HR1 dgn=LIB1 ndn=LIB2 svn=LIB3 mnc=5 mxc=10 sec=y`
- Unregister with the name, CICS-HR1.  
`bboc unregister rgn=CICS-HR1`
- Start a server transaction as BBO\$ for all service and program names under the registration name, CICS PAYR, with a WOLA group with 10 maximum connections, 5 minimum connections, and security propagation.  
`bboc start_srvr rgn=CICSPAYR dgn=LIB1 ndn=LIB2 svn=LIB3 mnc=5 mxc=10 sec=y`
- Stop the BBO\$ server transaction that is running under the registration name, CICS PAYR.

```
bboc stop_srvr rgn=CICSPAYR
```

- Start a server transaction as BBO\$ for the service and program names that start with PAYR under the register name, CICSPAY1, with a WOLA group with 10 maximum connections, 5 minimum connections, and security propagation.

```
bboc start_srvr rgn=CICSPAY1 dgn=LIB1 ndn=LIB2 svn=LIB3 mnc=5 mxc=10 sec=y svc=PAYR*
```

- Start a server transaction under the transaction ID, PAY2, and register with the name, PAYROLL2, for all service and program names in a WOLA group with 10 maximum connections, 5 minimum connections, basic tracing, and security propagation.

```
bboc start_srvr rgn=PAYROLL2 dgn=LIB1 ndn=LIB2 svn=LIB3 mnc=5 mxc=10 sec=y stx=PAY2 trc=1
```

- Start a server transaction under the transaction ID, PAY3, and the link transaction ID of PY3L. Register with the name, PAYROLL3, for service and program names that start with PAYRL3 in a WOLA group with 10 maximum connections, 5 minimum connections, basic tracing, and security propagation.

```
bboc start_srvr rgn=PAYROLL3 dgn=LIB1 ndn=LIB2 svn=LIB3 mnc=5 mxc=10 sec=y svc=PAYRL3*  
stx=PAY3 ltx=PY3L trc=1
```

### Automatically running a BBOC command during CICS startup

Two CICS Program List Table Post-Initialization (PLTPI) programs, BBOACPLT and BBOACPL2, are provided as samples on GitHub. For more information, see “Optimized local adapters samples for Liberty” on page 1691.

- To start the optimized local adapters TRUE when CICS starts, add BBOACLPT as phase 2 or phase 3 entries in your CICS PLT.
- To issue a BBOC command using INITPARM data when CICS starts, add BBOACPL2 as phase 2 or phase 3 entries in your CICS PLT.

You can pass a string of commands up to the CICS limit of 60 characters inside the INITPARM. The following sample INITPARM string calls BBOACPL2 and passes a request to start a link server under the register name PAYROLL, with WOLA group names of LIB1, LIB2, and LIB3. By specifying SVC=\*, this link server receives requests for all service names.

```
INITPARM=(BBOACPL2='STA RGN=PAYROLL DGN=LIB1 NDN=LIB2 SVN=LIB3 SVC=*')
```

The command string can be any BBOC command, such as REG in the following sample INITPARM string. When CICS starts, the string creates a registration under the name LIBAPP that consists of 10 minimum connections and 100 maximum connections.

```
INITPARM=(BBOACPL2='REG RGN=LIBAPP DGN=LIB1 NDN=LIB2 SVN=LIB3 MNC=10 MXC=100')
```

If you create a registration when CICS starts, do not use the Register API in your applications. Instead, immediately use the other APIs, such as Invoke or Connection Get.

**Important:** You can use only one INITPARM string per BBOACPL2 program.

If you use the PLT programs to automatically create a registration or a link server, be sure to unregister or stop the server before you shut down CICS to avoid a delay while CICS cancels any remaining optimized local adapters transactions. You can remove the optimized local adapters resources in the following ways:

- Run BBOC STOP\_SERVER for all CICS link servers or run BBOC URG for all registrations.
- Purge the BBO\$ tasks.
- Write a Program List Table (PLT) shutdown program that runs the EXEC CICS LINK command to BBOACNTL for each link server that passes the STOP\_SERVER string.
- Issue the following command: CEMT P SHUT, IMMED

## Link server transaction for CICS: BBO\$

The BBO\$ CICS transaction supports calls from the Liberty server to CICS. The BBO\$ transaction is a non-workstation transaction that represents an instance of a server task that is started with the BBOC START\_SRVR operation for a certain register name and service name. This server task provides program link invocation capability, which is the ability to start an existing CICS program from the Liberty server over the optimized local adapter APIs.

You can override the name of the transaction, BBO\$, by specifying `STX=name` on the BBOC START\_SRVR command. The new transaction name must be defined to CICS with the same program name and attributes as BBO\$. For more information, see “Optimized local adapter definitions for CICS” on page 1705.

## Program link invocation transaction for CICS: BBO#

The BBO# CICS transaction supports calls from the Liberty server to CICS. The BBO# transaction is a non-workstation transaction that represents an instance of a task that the link server task, BBO\$, starts to invoke a program link. The BBO\$ transaction initiates a BBO# for each CICS program link request from a Liberty server application.

You can override the name of the transaction, BBO#, by specifying `LTX=name` on the BBOC START\_SRVR command. The new transaction name must be defined to CICS with the same program name and attributes as BBO#. For more information, see “Optimized local adapter definitions for CICS” on page 1705. Alternatively, the Liberty server application can pass the new transaction name to CICS using the JCA `setLinkTaskTransid` method.

## Registering an external address space with a local Liberty server using optimized local adapters:



For WebSphere optimized local adapters (WOLA) to make an outbound call to your local optimized local adapter group or an inbound call to a Liberty server, you must bind the current address space to the Liberty server and establish connection attributes using the Register API.

### Before you begin

Enable the Liberty server environment to use WOLA. For more information, see “Enabling the Liberty server environment to use optimized local adapters” on page 1697.

The Liberty server must be active on the same z/OS image that the register request originates from.

If you are using the Customer Information Control System (CICS), enable optimized local adapters support in CICS. For more information, see “Enabling support for Liberty optimized local adapters in CICS” on page 1703. Activate the task-related user exit (TRUE) program before you make a connection between CICS and the Liberty server.

### Procedure

1. Decide which parameters to use when you register the address space using the Register API, BBOA1REG.

The API accepts parameters for the following items:

- The three parts of the WOLA group name that you specified when you added the feature to the `server.xml` file
- The register name
- The minimum number of initial connections
- The maximum number of connections

- Registration flag words to specify tracing behavior

For inbound calls to the Liberty server, a security context that contains the user ID of the address space that makes the request is always propagated to the Liberty server. For CICS, the `reg_flag_C2Wprop` registration flag propagates the user ID of the CICS task rather than the user ID from the address space.

For outbound calls from the Liberty server, the `reg_flag_W2Cprop` registration flag tells the Liberty server to propagate the user ID to CICS. CICS then attempts to start the target program with that user ID.

For more information about API parameters, see “Optimized local adapters APIs on Liberty for z/OS” on page 2079 and “Securing optimized local adapters on Liberty for z/OS” on page 1949.

2. Verify that another optimized local adapter group that this address space is connected to is not already using the selected register name. If the register name is used by another optimized local adapter group, an error return code is passed back, and the register request fails.
3. Call the Register API for your caller from the native-language application in the client address space using the parameters that you selected.  
A 0 return and reason code indicates that the client address space is now bound to the Liberty server.

## Results

The passed register name string is reserved in the current address space. No other register calls can be made with this token until an Unregister API call is received for it.

**Important:** If you use the minimum connections setting on this call, the result is a pool of connections that are pre-established with the target server and wait for requests.

A registration entry context or control block is also created and associated with the register name string. Each unique register name has a register context. Multiple register names with the same address space and thread can bind with one or more Liberty optimized local adapter groups.

## What to do next

You can use the registration to make inbound and outbound calls between the Liberty environment and the external address space. For more information, see “Developing applications that use optimized local adapters on Liberty” on page 2073.

## Administering web applications on Liberty

Liberty provides support to the web applications using Liberty features such as `servlet-3.0`, `servlet-3.1`, `jsp-2.2`, and other features.

### Procedure

Specify when servlets are loaded and initialized.

#### Specifying when servlets are loaded and initialized

By default, Liberty defers servlet loading until a request is received for the associated web application. You can override this default behavior by specifying the web container `deferServletLoad` attribute to `false`.

#### About this task

The servlet specification defines the **load-on-startup** servlet attribute, which is specified in the `web.xml` file of a web application. If a servlet has a non-negative value for the **load-on-startup** attribute, the servlet must be loaded and initialized when the web application is deployed. Liberty optimizes server start time and memory use by not starting a servlet until a request is received for the web application.

You can override this deferral so that your servlets are loaded and initialized when the web application is installed, rather than waiting for the first request for the application.

## Example

To configure the server to load servlets when a web application is installed, add the following line to the `server.xml` configuration file or a file that it includes:

```
<webContainer deferServletLoad="false"/>
```

This setting applies to all web applications installed in the server.

## Configuring Cross Origin Request Sharing on a Liberty server

8.5.5.9

You can enable Cross Origin Request Sharing (CORS) for your web applications on a Liberty server.

### About this task

Enabling CORS will allow JavaScript clients to make requests against your application on the Liberty server even if the client and the server are on two different domains. Web browsers prevent these requests due to same-origin policy.

### Procedure

1. Ensure the server configuration has all features needed for your deployed application, such as `servlet-3.0`, `jaxrs-1.1`, and so on. Also ensure the ports and user registry settings are correct for the deployed application.
2. Add the CORS service setting to the `server.xml` file. The `cors` element defines the CORS settings for the URL being setup in the domain.

### Example

Here is an example of a CORS configuration for a web application at the `sampleApp/path` context root.

```
<cors domain="/sampleApp/path"
  allowedOrigins="https://alice.com:8090"
  allowedMethods="GET, DELETE, POST"
  allowedHeaders="accept, MyRequestHeader1"
  exposeHeaders="MyResponseHeader1"
  allowCredentials="true"
  maxAge="3600" />
```

Here is an example of a CORS configuration for the RESTful endpoint `/ibm/api/collective`. This setting will apply to all the endpoint paths which start with `/ibm/api/collective` including `ibm/api/collective/docs`.

```
<cors domain="/ibm/api/collective"
  allowedOrigins="https://alice.com:8090"
  allowedMethods="GET, DELETE, POST"
  allowedHeaders="accept, MyRequestHeader1"
  exposeHeaders="MyResponseHeader1"
  allowCredentials="true"
  maxAge="3600" />
```

## Configuring Liberty for Servlet 3.1

You can configure Liberty for the Servlet 3.1 feature, which provides full support for the Servlet 3.1 specification.

## About this task

To configure a Liberty server to run an application that is enabled for Servlet 3.1, you must set the `<servlet-3.1>` feature.

## Procedure

Update the `server.xml` file to add the `<servlet-3.1>` feature. For example:

```
<featureManager>
  <feature>servlet-3.1</feature>
</featureManager>
```

### Important:

- The `websocket-1.0` and `websocket-1.1` features require the `servlet-3.1` feature and as a result, configuring the `websocket-1.0` or `websocket-1.1` feature causes the `servlet-3.1` feature to load.
- You can use Java EE 6 features, such as `jsp-2.2` and `jsf-2.0`, with the `servlet-3.1` feature. However, you cannot use a Java EE 6 feature to exploit Servlet 3.1 features.
- You can choose between the Servlet 3.0 and Servlet 3.1 feature implementations for each server instance, but you must consider any behavior changes. If required behavior is contained only in the Servlet 3.1 feature, then you must use the Servlet 3.1 feature. If an existing application would be adversely impacted by behavior changes in the Servlet 3.1 feature, then use the Servlet 3.0 feature to preserve the existing behavior for that application.
- It is not possible to use both the Servlet 3.0 and Servlet 3.1 features in the same Liberty server. If both features are configured, it will produce an error. Read the Servlet 3.1 behavior changes topic to learn about changes from Servlet 3.0 and Servlet 3.1.

## Results

The Servlet-3.1 feature is enabled and loads in the Liberty server at run time.

### Servlet 3.1 behavior changes:

The Servlet 3.1 implementation contains behavior changes that might cause an application that was written for Servlet 3.0 to behave differently or fail when you use the Servlet 3.1 feature.

You can choose between the Servlet 3.0 and Servlet 3.1 feature implementations for each server instance, with consideration for behavior changes. If the required behavior is contained in the Servlet 3.1 feature only, then you must use the Servlet 3.1 feature. If an existing application would be adversely impacted by behavior changes in the Servlet 3.1 feature, then using the Servlet 3.0 feature preserves the existing behavior for that application. It is not possible to use both the Servlet 3.0 and Servlet 3.1 features in the same server. It is an error to configure both features. If you configure both features, neither servlet feature is loaded.

The behavior changes are introduced for three reasons:

- Changes that are required by clarifications in the Servlet 3.1 specification.
- Changes that are required for the Servlet 3.1 implementation to pass the Servlet 3.1 Technology Compatibility Kit (TCK).
- Changes to improve the servlet implementation.

### Programmatically added servlets, filters, and listeners

A clarification from the Servlet 3.1 specification now makes it illegal for a `ServletContextListener` to programmatically configure servlets, filters, or listeners if the `ServletContextListener` was not declared in the `web.xml` file or `web-fragment.xml` file or was not annotated with `@WebListener`. As a result, any call

on the ServletContext to perform such programmatic configuration results in an UnsupportedOperationException.

### **Forward after asynchronous processing is started**

In the Servlet 3.0 implementation, a response is always closed before the forward method of the RequestDispatcher interface returns. However, due to a clarification in the Servlet 3.1 specification, the Servlet 3.1 implementation does not close or flush the response before the forward method of the RequestDispatcher interface returns, if the request is put into the asynchronous mode. This change might affect existing 3.0 applications, which add response output on return from forward because such response data is now sent, whereas in Servlet 3.0, it was not.

### **URL pattern clashes**

In Servlet 3.0, an application would start successfully even when a URL pattern was mapped to multiple servlets. However, due to a clarification in the Servlet 3.1 specification, the application must fail to start. In the Liberty Servlet 3.1 implementation, a message is output and the application fails to start:

```
SRVE9016E: Unable to insert mapping [{0}] for servlet named [{1}]. The URL pattern is already defined for servlet named
```

Explanation: There is an application error. A servlet mapping URL pattern should not map to multiple servlets.

User action: Change the URL pattern for the servlet mapping.

### **ServletContext.getMinorVersion()**

In the Servlet 3.0 feature implementation, this API returns 0.

In the Servlet 3.1 feature this API now returns 1.

### **ServletContext.getServerInfo()**

In the Servlet 3.0 feature implementation, this API returns SMF WebContainer.

In the Servlet 3.1 feature this API now returns IBM WebSphere Liberty/8.5.5.<x>, where <x> is the WebSphere Application Server fix pack number.

### **ServletResponse.reset()**

You can use ServletResponse.reset() to clear any buffered response data, the status code, and response headers when a response is not already committed. If the Servlet 3.1 feature is being used, this method also clears any record of ServletResponse.getWriter() or ServletResponse.getOutputStream() that were previously called.

### **X-Powered-By header**

In the Servlet 3.0 feature implementation, the X-Powered-By header is set to Servlet/3.0. In the Servlet 3.1 feature implementation, the X-Powered-By header is set to Servlet/3.1.

### **Resource reference injection target merging**

In the Servlet 3.0 specification, the <injection-target> elements of a resource reference that is defined in a web-fragment.xml file are added only to the parent web.xml file if the web.xml resource reference definition with the same name has no <injection-target> elements. In the Servlet 3.1 specification, it is clarified that all <injection-target> elements in web-fragment.xml descriptors are added to the parent web.xml descriptors list of <injection-target> elements for a resource reference of the same name. When the Servlet 3.1 feature is in use, this feature might change existing application function by activating

injection targets that were previously excluded from the web.xml file.

### **Tolerance of duplicate elements in web descriptors**

In the Servlet 3.1 specification, it was clarified that a web.xml file cannot contain two <absolute-ordering> elements. Deployment of an application with multiple <absolute-ordering> elements fails. Additionally, web-fragment.xml descriptors cannot contain two <ordering> elements. Deployment of an application with multiple <ordering> elements fails. Previously, the deployment would not fail, but the function of the elements might be indeterminate.

### **Web fragment ordering change in metadata - complete cases**

The processing of the <absolute-ordering> element is changed in cases where a web.xml descriptor is marked metadata-complete="true". Previously in metadata-complete="true" cases, all web fragment archives would be used. When the Servlet-3.1 feature is in use, the <absolute-ordering> element in metadata-complete cases is considered to be complete. This change results in fragments that are not listed in the <absolute-ordering> element to be excluded from processing.

### **AsyncContext.dispatch()**

When AsyncContext.dispatch() is used (for example, with no parameters), the request is dispatched to the original URL. With the Servlet-3.0 feature in use, if a query string was included with the original request, this is made available to the dispatched resource. However, when the Servlet 3.1 feature in use, if a query string was provided to the dispatching resource, it is this query string that is made available to the dispatched resource. For example:

Request for /FirstResource?param=One

First Resource:

```
getParameter("param") returns "One"
forward request to /SecondResource?param=Two
```

SecondResource

```
getParameter(param) returns "Two"
ac.start()
ac.dispatch() dispatches to /FirstResource
```

First Resource

```
Servlet-3.0 feature : getParamter("param") returns "One"
Servlet-3.1 feature : getParameter("param") returns "Two"
```

This change was required by the Servlet 3.1 TCK.

Obtaining the request or response object after an AsyncContext.dispatch() or AsyncContext.complete() is not permitted and results in the following exception being thrown:

```
java.lang.IllegalStateException: SRVE9015E: Cannot obtain the request or response object after an AsyncContext.dispatch() o
at com.ibm.ws.webcontainer31.async.AsyncContext31Impl.getRequest(AsyncContext31Impl.java:72)
[...]
```

### **SessionCookieConfig.setComment()**

According to the Java Servlet 3.1 Specification, this API returns an illegalStateException if it is called after the ServletContext completes initialization, and the Servlet 3.1 feature follows this required behavior. However, the Servlet 3.0 feature does not prevent use of this API after the context is initialized and as a result, applications that depend on the Servlet 3.0 feature behavior will not work with the Servlet 3.1 feature.

### **sendRedirect(java.lang.String location) API**

The sendRedirect(java.lang.String location) API accepts relative URLs; however, the servlet container must convert the relative URL to an absolute URL before it can send the response to the client. If the

location is relative without a leading '/' (folder/default.jsp), the container interprets it as relative to the current request URI. If the location is relative with a leading '/', the container interprets it as relative to the servlet container root.

For example, if the redirection location that is provided by application is folder/default.jsp, with no leading '/', and the inbound request URL is http://host:port/context\_root/folder or http://host:port/context\_root/folder/, the request is redirected to http://host:port/context\_root/folder/folder/default.jsp, which is relative to the current request URI.

This behavior is found in the Servlet 3.0 feature when the `com.ibm.ws.webcontainer.redirectwithpathinfo` property is set to **true**. This property is ignored in the Servlet 3.1 feature and the behavior defaults, as described.

## Default error pages

The IBM extended function is the ability to specify a default error page with a web extension, such as `ibm-web-ext.xml`.

As a function of Servlet 3.0 and higher, default error pages are a modification of the ability to specify error pages. As with normal (non-default) error pages, default error pages are specified in web module descriptors (`web.xml`), and in web fragment descriptors (`web-fragment.xml`).

Normal (non-default) error pages specify either an exception-type or an error-code. A default error page omits both exception-type and error-code. A default error page is used when a servlet throws an exception or sets an error-code result and no configured error page matches the type of the exception or matches the set error code.

The ability to define default error pages is provided by the Servlet 3.0 specification, and is supported by the Servlet 3.0 schemas. Default error pages are error pages that do not contain an **exception-type** or an **error-code** element, according to the Servlet 3.1 specification.

Examples of error pages and default error pages follow.

### Default error page precedence rules

Three rules apply for determining precedence for default error pages in the `web.xml`, `web-fragment.xml`, and `ibm-web-ext.xml` files.

- Rule 1: `web.xml` and `web-fragment.xml` files.

When a default error page is specified in the `web.xml` file, it overrides (masks) any default error page that is specified in a `web-fragment.xml` file. Also, there is no error if, in addition, multiple `web-fragment.xml` files specify default error pages.

- Rule 2: `web-fragment.xml` and `web-fragment.xml`.

When a default error page is not specified in the `web.xml` file, an error condition exists if different default error pages are specified by two or more `web-fragment.xml` files.

- Rule 3: `ibm-web-ext.xml` and `web.xml` or `web-fragment.xml` files.

The rule of precedence between the `ibm-web-ext.xml` file and either the `web.xml` or `web-fragment.xml` files depends on the web container feature level.

When the web container feature level is 3.0, a default error page that is defined by an `ibm-web-ext.xml` file has precedence over a default error page that is defined in `web.xml` or `web-fragment.xml` files.

**Note:** When the web container uses feature level 3.0, you cannot use Servlet 3.1 schemas. Refer to the rule on using default error pages for servlet 3.0 schemas.

When the web container feature level is 3.1 or higher, a default error page that is specified by `web.xml` or `web-fragment.xml` file has precedence over a default error page that is specified in the `ibm-web-ext.xml` file.

## Schema rules

Two rules apply for whether default error pages are processed in `web.xml` or `web-fragment.xml` files. The rules depend on the web container feature version, which Servlet schema is in use, and the setting of a Java custom property.

These rules arose because IBM WebSphere Application Server traditional V8.0, did not support default error pages in the V8.0 general availability release. Support for default error pages was added to WebSphere Application Server traditional, in a service pack, by APAR PM94199.

Support for default error pages was added to WebSphere Application Server Liberty, in a service pack, by APAR PI05845. Because these updates are a change of externally visible function, the new function is disabled by default and must be enabled by a Java system property.

- Rule 1: Default error pages using Servlet 3.0 schema and using web container feature version 3.0.

When the web container feature version is 3.0 and a default error page is specified in `web.xml` or `web-fragment.xml` files that use a Servlet 3.0 schema, the default error pages are processed only if `com.ibm.ws.webcontainer.allowdefaulterrorpage` Java system property is set to **true**. When the Java system property is not set, or is not set to **true**, the default error page is ignored. A default error page that is specified by the `ibm-web-ext.xml` file is used.

- Case 2: Default error pages by using web container feature version 3.1.

When the web container feature version is 3.1 or higher, a default error page that is specified in the `web.xml` file or the `web-fragment.xml` file is always processed, regardless of what servlet schema version is used, and regardless of whether the Java custom property is set.

This case occurs when a descriptor uses a Servlet 3.1 schema, since the processing of a descriptor that uses a Servlet 3.1 schema requires web container feature version 3.1.

**Attention:** Web fragments were not added until Servlet 3.0. The `web-fragment.xml` file has no schema from Servlet 2.5.

## Error page and default error page examples

A default error page that is defined in an `ibm-web-ext.xml` file:

```
<?xml version="1.0" encoding="UTF-8"?>
<web-ext xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-web-ext_1
  version="1.0">

  <default-error-page uri="/ExtErrorPage.html"/>
</web-ext>
```

An error-code error page element, which is defined in either the `web.xml` file or `web-fragment.xml` file:

```
<error-page>
  <error-code>404</error-code>
  <location>/ErrorCodeErrorPage.html</location>
</error-page>
```

An exception-type error page element, which is defined in either the `web.xml` file or `web-fragment.xml` file:

```
<error-page>
  <exception-type>javax.servlet.ServletException</exception-type>
  <location>/ExceptionTypeErrorPage.html</location>
</error-page>
```

A default error page element, which is defined in either the `web.xml` file or `web-fragment.xml` file:

```

<error-page>
  <location>/DefaultErrorPage.html</location>
</error-page>

```

### Schema examples

Example header of a web.xml file that uses a Servlet 2.5 schema:

```

<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://java.sun.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/javaee http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd"
  version="2.5">

```

Example header of a web.xml file that uses a Servlet 3.0 schema:

```

<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://java.sun.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/javaee http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd"
  version="3.0">

```

Example header of a web.xml file that uses a Servlet 3.1 schema:

```

<?xml version="1.0" encoding="UTF-8"?>
<web-app
  xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  version="3.1">

```

Example header of a web-fragment.xml file that uses a Servlet 3.0 schema:

```

<?xml version="1.0" encoding="utf-8"?>
<web-fragment xmlns="http://java.sun.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/javaee http://java.sun.com/xml/ns/javaee/web-fragment_3_0.xsd"
  version="3.0">

```

Example header of a web-fragment.xml file that uses a Servlet 3.1 schema:

```

<?xml version="1.0" encoding="utf-8"?>
<web-fragment xmlns="http://java.sun.com/xml/ns/javaee"
  xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee http://xmlns.jcp.org/xml/ns/javaee/web-fragment_3_1.xsd"
  version="3.1">

```

### Servlet 3.1 feature functions:

The product supports a subset of Servlet 3.1 functions. View the clarifications and descriptions of some of the functions available.

Descriptions of the new Servlet 3.1 functions are provided in the specification and are not described here. However, additional considerations for the Servlet 3.1 feature are as follows:

#### Asynchronous I/O

A new feature of the Servlet 3.1 feature specifies that when the non-blocking read is started, any resource during the remaining request lifetime cannot call APIs, which can result in a blocking read. For example, for a POST request after the read listener is set by the resource, any subsequent call to `getParameter()` and `getPart()` API results in an `IllegalStateException`.

You must consider setting timeout with the `AsyncContext.setTimeout` API when you work with async servlets, otherwise the container default value (for example, 30 seconds) is used. The timeout resets each time async starts using the `ServletRequest.startAsync` API is called and expires when the `AsyncContext.complete` API is not called within the timeout period that follows the last time async started. When you use the async I/O support that is provided by the Servlet 3.1 feature, set the timeout

value with the `AsyncContext.setTimeout` API to also allow for async I/O to complete. Completion depends on other external factors, such as environment or network speed.

## Upgrade processing

| **Important:** Use the `ServletOutputStream` class with the `WriteListener` interface and the  
| `ServletInputStream` class with the `ReadListener` interface. Do not use these classes with the  
| `ObjectInputStream` class or the `ObjectOutputStream` class. These classes circumvent some of the required  
| checks for the `ReadListener` and `WriteListener` interfaces, mainly the `isReady` checks, and can cause  
| unexpected behavior.

| Upgrade processing is a Servlet 3.1 feature that has non-blocking read and write capability. When the read or write operations are async, there are no limits on how much time the server waits for the operation to complete. You can set the timeouts with the web container custom properties in the `server.xml` file, such as `upgradereadtimeout` and `upgradewritetimeout`. See the following example of a timeout of 5 seconds:

```
<webContainer upgradereadtimeout="5000" />  
<webContainer upgradewritetimeout="5000" />
```

The request must not be upgraded by using the upgrade feature for Servlet 3.1 when the request is being handled by async servlet.

The application that supports the Servlet 3.1 feature for upgrade requires that the connection on the request remains open between the client and the application that hosts the upgrade. If the application does not initiate the `WebConnection.close()` when the upgrade processing is complete from its handler or any other resources, such as `ReadListener` or `WriteListener`, the TCP connection remains open until the server recycles.

When you use an `UpgradeHandler` and a `ReadListener` from the Servlet 3.1 feature, the `ReadListener.onAllDataRead` method is invoked only when the client closes the connection to the server that hosts the upgraded application. The Javadoc for `onReadListener.onAllDataRead` returns the following message:

Invoked when all data for the current request is read.

In the Upgrade case, the server does not know the end of the data because upgraded data is not delimited the way that HTTP request body data is. Aside from when the client connection closes, there is no determination for the end of the data.

## Form based authentication

After successful authentication, a client is redirected to the resource of the original request. The Servlet 3.1 specification specifies: To improve the predictability of the HTTP method of the redirected request, containers should redirect using the 303 (SC\_SEE\_OTHER) status code, except where interoperability with HTTP 1.0 user agents is required; in which cases the 302 status code should be used. The Servlet-3.1 feature maintains interoperability with HTTP 1.0 user agents and always uses the 302 status code. For more information on configuring Servlet 3.1 for security, read the [Configuring Liberty for Servlet 3.1](#) topic.

## Large post data

The addition of the `ServletRequest.getContentLengthLong()` API requires support for receiving post data of a length greater than `Integer.MAX_VALUE` and cannot be fully accommodated in a single-byte array or string.

This addition has implications when you obtain post data content that use APIs that return content in a string or `byte[]`. For example, the `javax.servlet.ServletRequest` methods for accessing parameters:

```
String getParameter(String name)
String[] getParameterValues()
Map<String,String> getParameterMap()
```

It is possible to send post data that contains multiple parameters, which when combined, have a length of greater than `Integer.MAX_VALUE`. However, each individual parameter name and parameter value must be less than `Integer.MAX_VALUE` in length.

Sending a large amount of post data include these additional considerations:

- You must send post data in chunks of less than `Integer.MAX-VALUE` in length.
- Post data that is processed by the web container, such as parameters or parts, must be fully read before processing starts. The post data might impose significant memory requirements for large post data because it might require as much memory as double the size of the post data in order for web container processing to be successful.

## Configuring Liberty for Expression Language 3.0



8.5.5.5

You can configure Liberty for the Expression Language (EL) 3.0 feature, which provides full support for the EL 3.0 specification.

### About this task

To configure a Liberty server to run an application that is enabled for EL 3.0, you must set the `<el-3.0>` feature.

### Procedure

Update the `server.xml` file to add the `<el-3.0>` feature. For example:

```
<featureManager>
  <feature>el-3.0</feature>
</featureManager>
```

### Important:

- The EL 3.0 feature does not require any additional features. You can configure it independently of JavaServer Pages (JSP) 2.3.
- The JSP 2.3 feature requires the EL 3.0 feature. When you configure the JSP 2.3 feature, the EL 3.0 feature also loads into the server run time.
- You can use other Java EE 6 features, such as JSF 2.0 and CDI 1.0, with the EL 3.0 feature.
- You can choose between EL 3.0 and EL 2.2 (included in the JSP 2.2 feature) for each server instance, but you must consider any behavior changes. If the required behavior is contained only in the EL 3.0 feature, then you must use the EL 3.0 feature. If an existing application would be adversely impacted by behavior changes in the EL 3.0 feature, then use the EL 2.2 feature (included in JSP 2.2) to preserve the existing behavior for that application.
- It is not possible to use both the EL 3.0 feature and JSP 2.2 (includes EL 2.2) features in the same Liberty server. If both features are configured, it produces an error:  
CWWKF0033E: The singleton features com.ibm.websphere.appserver.javax.el-2.2 and com.ibm.websphere.appserver.javax.el-3

See  [8.5.5.5](#) “Expression Language 3.0 feature functions” on page 1722 to learn about changes in the EL 3.0 feature, compared to the EL 2.2 feature.

### Results

The EL 3.0 feature is enabled and loads in the Liberty server at run time.

## Expression Language 3.0 feature functions: 8.5.5.5

The Expression Language (EL) 3.0 feature provides full support for the EL 3.0 specification.

Descriptions of EL 3.0 functions are provided in the EL 3.0 specification and are not fully described here. However, some of the key enhancements include the following:

- EL 3.0 is now available as a separate feature and you can configure it independently of JavaServer Pages (JSP) 2.3.
- Add support for Lambda expressions (value expression with parameters). For more information, see Section 1.20 of the EL 3.0 specification.
- Addition of operations on collections objects. For more information, see Chapter 2.0 of the EL 3.0 specification.
- New operators:
  - String concatenation. For more information, see section 1.8 of the EL 3.0 specification.
  - Assignment. For more information, see section 1.13 of the EL 3.0 specification.
  - Semi-colon. For more information, see section 1.14 of the EL 3.0 specification.
  - Field and Methods. For more information, see Section 1.22 of the EL 3.0 specification.

**Important:** There is a change in the EL 3.0 feature that might break existing applications. The default coercion for nulls to non-primitive types (except String) returns nulls. For example, a null that is coerced to a Double now returns a null value, whereas before it returned 0.0. The following code example describes this scenario:

```
Integer number=null;  
factory.coerceToType(number, java.lang.Double.class)
```

## Configuring Liberty for JavaServer Faces 2.2

8.5.5.6

You can configure Liberty for the JavaServer Faces (JSF) 2.2 feature, which provides full support for the JSF 2.2 specification.

### About this task

The Liberty JSF implementation is based on the MyFaces open source implementation. To configure a Liberty server to run an application that is enabled for JSF 2.2, you must set the <jsf-2.2> feature.

### Procedure

Update the `server.xml` file to add the <jsf-2.2> feature. For example:

```
<featureManager>  
  <feature>jsf-2.2</feature>  
</featureManager>
```

### Important:

Consider the following points when you use JavaServer Faces 2.2:

- JSF 2.2 feature does not implicitly load the bean validation feature like the JSF 2.0 feature does. When you migrate your application from JSF 2.0 to JSF 2.2, and your application uses bean validation, you must also enable the `beanValidation-1.1` feature.
- The JSF 2.2 feature requires the `servlet-3.1`, `jsp-2.3`, `timedexit-1.0`, and `el-3.0` features. When the JSF 2.2 feature is enabled in the `server.xml` file, each of these features is also enabled.
- You cannot run the JSF 2.2 feature with Java EE 6 features; for example, `servlet-3.0`, `jsp-2.2` and `cdi-1.0`.

- You can choose between the JSF 2.0 and JSF 2.2 feature implementations for each server instance, but you must consider any behavior changes. If the required behavior is contained only in the JSF 2.2 feature, then you must use the JSF 2.2 feature. If an existing application would be adversely impacted by behavior changes in the JSF 2.2 feature, then use the JSF 2.0 feature to preserve the existing behavior for that application.
- It is not possible to use both the JSF 2.0 and JSF 2.2 features in the same Liberty server. If both features are configured, it produces an error:  
CWWKF0033E: The singleton features jsf-2.0 and jsf-2.2 cannot be loaded at the same time. The configured features jsf-2.0 and jsf-2.2 cannot be loaded at the same time.
- JSF 2.2 is compatible with earlier releases, such as JSF 2.1 and JSF 2.0; however, consider the following exceptions:
  - An error in previous versions of the JSF specification caused exceptions to be swallowed that now are propagated to the exception handler. Read Backward Compatibility with Previous Versions in the overview section of the JSF 2.2 specification.
  - Changes made to the specification for Composite Component Attribute ELResolver and Composite Component Metadata. Read Backward Compatibility with Previous Versions in the overview section of the JSF 2.2 specification.

## Results

The JSF 2.2 feature is enabled and loads in the Liberty server at run time.

## What to do next

To use the FlowBuilder API to create Flows with FlowBuilder annotations, it is required that the relevant CDI producer method is declared within a managed bean or a session bean class. To ensure that the class is managed correctly by CDI, define the producer method class as a managed bean (by giving it a scope), or set CDI bean-discovery-mode to all. You can set the CDI bean-discovery-mode to all in the beans.xml file in your web archive:

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee http://xmlns.jcp.org/xml/ns/javaee/beans_1_1.xsd"
  bean-discovery-mode="all">
</beans>
```

## JavaServer Faces 2.2 feature functions: 8.5.5.6

The JavaServer Faces (JSF) 2.2 feature provides full support for the JSF 2.2 specification.

Descriptions of JSF 2.2 functions are provided in the JSF 2.2 specification and are not fully described here. However, some of the key enhancements are as follows:

- Faces Flows enables developers to logically group JSF views to represent modules of functions. Each module has a well-defined set of entry and exit points. Combining modules creates a flow of functions. An example of a flow of functions is an order checkout process. Read section 7.5 of the JSF 2.2 specification.
- Resource Library Contracts enable resource libraries to reside in the contracts directory of the web-app root directory, or in the META-INF/contracts entry name in the JAR file. Read section 10.1.3 of the JSF 2.2 specification.
- JSF 2.2 introduced the ability for applications to use stateless views. Read section 7.8.1.1 of the JSF 2.2 specification.
- JSF 2.2 can handle HTML5 attributes through pass-through elements and pass-through attributes. Read section 10.1.4 of the JSF 2.2 specification.

## Configuring Liberty for JavaServer Pages 2.3



8.5.5.5

You can configure Liberty for the JavaServer Pages (JSP) 2.3 feature, which provides full support for the JSP 2.3 specification.

### About this task

To configure a Liberty server to run an application that is enabled for JSP 2.3, you must set the `<jsp-2.3>` feature.

### Procedure

Update the `server.xml` file to add the `<jsp-2.3>` feature. For example:

```
<featureManager>
  <feature>jsp-2.3</feature>
</featureManager>
```

### Important:

- The `jsp-2.3` feature requires both the `servlet-3.1` and `el-3.0` features and when configured, causes these features to load.
- You cannot use `jsp-2.3` with the `servlet-3.0` feature.
- You can use other Java EE 6 features, such as JSF 2.0 and CDI 1.0, with the JSP 2.3 feature.
- You can choose between the JSP 2.2 and JSP 2.3 feature implementations for each server instance, but you must consider any behavior changes. If the required behavior is contained only in the JSP 2.3 feature, then you must use the JSP 2.3 feature. If an existing application would be adversely impacted by behavior changes in the JSP 2.3 feature, then use the JSP 2.2 feature to preserve the existing behavior for that application.
- It is not possible to use both the JSP 2.2 and JSP 2.3 features in the same Liberty server. If both features are configured, it produces an error:

CWWKF0033E: The singleton features jsp-2.3 and jsp-2.2 cannot be loaded at the same time. The configured features jsp-2.3



8.5.5.5

“JavaServer Pages 2.3 feature functions” to learn about changes in the JSP 2.3 feature.

### Results

The JSP 2.3 feature is enabled and loads in the Liberty server at run time.

### JavaServer Pages 2.3 feature functions: 8.5.5.5

The JavaServer Pages (JSP) 2.3 feature provides full support for the JSP 2.3 specification.

Descriptions of the new JSP 2.3 functions are provided in the JSP 2.3 specification and are not described here. However, the new specification additions are minor, as compared to the JSP 2.2 feature:

- Support for Expression Language (EL) 3.0
- Availability of Servlet 3.1 APIs to a JSP.
- There are no known behavior differences between JSP 2.2 and JSP 2.3 that directly prevent a JSP that runs with JSP 2.2 from successfully running with JSP 2.3. However, if a JSP uses Expression Language (EL) or Servlet API functions, you must consider the changes between Servlet 3.1 and Servlet 3.0, and between EL 3.0 and EL 2.2.

# Administering Contexts and Dependency Injection applications on Liberty



8.5.5.6

Liberty provides support for contexts and dependency injection in applications using the Liberty features `cdi-1.0` and `cdi-1.2`.

## Procedure

-  [8.5.5.6](#) “Configuring Liberty for Contexts and Dependency Injection 1.2”
-  [8.5.5.6](#) “Contexts and Dependency Injection 1.2 overview”
-  [8.5.5.6](#) “Contexts and Dependency Injection 1.2 behavior changes” on page 1726

## Configuring Liberty for Contexts and Dependency Injection 1.2



8.5.5.6

You can configure Liberty for the Contexts and Dependency Injection (CDI) 1.2 feature, which provides full support for the Contexts and Dependency Injection 1.2 specification.

### About this task

To configure the Liberty server to run an application that is enabled for CDI 1.2, you must set the `<cdi-1.2>` feature.

## Procedure

Update the `server.xml` file to add the `<cdi-1.2>` feature. For example:

```
<featureManger>
  <feature>cdi-1.2</feature>
</featureManger>
```

### Note:

- You can use other Java EE 7 features, such as `jsp-2.3` and `jsf-2.2` with the `cdi-1.2` feature. However, you cannot use Java EE 6 features such as `jsp-2.2` and `jsf-2.0` with the `cdi-1.2` feature.
- You can choose between the CDI 1.0 and CDI 1.2 feature implementations for each server instance, but you must consider the behavior changes. If the behavior is only contained in the CDI 1.2 feature, then you must use the CDI 1.2 feature. If an existing application might be adversely impacted by behavior changes in the CDI 1.2 feature, then use the CDI 1.0 feature to preserve the existing behavior for that application.
- It is not possible to use both the CDI 1.0 and CDI 1.2 features in the same Liberty server. If both features are configured, it produces an error. Read the CDI 1.2 behavior changes topic to learn about changes from CDI 1.0 to CDI 1.2.

## Results

The CDI 1.2 feature is enabled and loads in the Liberty server at run time.

## Contexts and Dependency Injection 1.2 overview



8.5.5.6

Liberty provides support for contexts and dependency injection in applications by using the Liberty features `cdi-1.0` and `cdi-1.2`.

The Contexts and Dependency Injection (CDI) 1.2 feature provides full support for the CDI 1.2 specification. Full descriptions of the CDI 1.2 functions are provided in the CDI 1.2 specification, see Contexts and Dependency Injection for the Java EE platform.

The set of services that are provided by the CDI 1.2 feature includes a well-defined lifecycle for stateful objects that are bound to lifecycle contexts and a typesafe dependency injection mechanism.

### **Using Contexts and Dependency Injection 1.2 with JavaServer Faces applications**

You can use the CDI 1.2 feature with the JavaServer Faces (JSF) 2.2 feature to enable JSF applications to take advantage of the sophisticated context and dependency injection model that is provided in the CDI 1.2 feature. This service is provided through integration with the Unified Expression Language (EL) which enables any contextual object to be used directly within a JSF or JavaServer Pages (JSP) page.

### **Using Contexts and Dependency Injection 1.2 with Enterprise JavaBeans (EJB)**

You can use the CDI 1.2 feature with the Enterprise JavaBeans (EJB) 3.2 feature to enhance the EJB component model with contextual lifecycle management. The services that are provided by the CDI 1.2 feature integrate the Java EE web tier with Java EE enterprise services. In particular, this enables EJB components to be used as JSF managed beans, thus integrating the programming models of EJB and JSF.

### **Using Contexts and Dependency Injection 1.2 with Servlet 3.1**

You can use the CDI 1.2 feature with the Servlet 3.1 feature to enable servlet applications to take full advantage of the services that are provided by the CDI 1.2 feature. Using both features enables contextual managed beans to be injected into servlet applications by using field, method or constructor injection. The CDI 1.2 feature also provides automatic registration of servlet listeners, filters, and interceptors.

### **Java Interceptors in Contexts and Dependency Injection 1.2 Applications**

The CDI 1.2 feature extends the Java model for interceptors. The CDI 1.2 feature provides the ability to associate interceptors with beans. The interceptors are bound by using typesafe interceptor bindings. This model can be extended to EJB beans when both the CDI 1.2 and EJB 3.2 features are loaded onto the Liberty server.

### **Contexts and Dependency Injection 1.2 behavior changes**



8.5.5.6

The Contexts and Dependency Injection (CDI) 1.2 implementation contains some behavior changes that might cause an application that was migrated from CDI 1.0 to behave differently or fail on CDI 1.2.

You can choose between the CDI 1.0 and CDI 1.2 feature implementations for each server instance, with consideration for behavior changes. If the required behavior is contained in the CDI 1.2 feature only, then you must use the CDI 1.2 feature. If an existing application might be adversely impacted by behavior changes in the CDI 1.2 feature, then by using the CDI 1.0 feature the existing behavior is preserved for that application. It is not possible to use both the CDI 1.0 and CDI 1.2 features in the same server as the features are not compatible. If you configure both features, the server produces a configuration error.

The CDI 1.0 feature is built on Apache OpenWebBeans implementation of CDI. The CDI 1.2 feature is built on the Weld implementation of CDI. The behavior changes introduced are due to the differences in the two implementations.

## The conversation ID CID

In the CDI 1.0 implementation, the CID is globally unique. In CDI 1.2, it is unique per HTTP session. This behavior is in line with the CDI specification and is a convention that is chosen by the Weld. To get a globally unique CID, the CID must be specified at conversation start by calling `Conversation.begin`.

## Referencing schemas in the beans.xml file

In a CDI 1.2 implementation, here is an example of a schema that is referenced in the beans.xml file:

```
xmlns="http://xmlns.jcp.org/xml/ns/javaee"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee http://xmlns.jcp.org/xml/ns/javaee/beans_1_1.xsd"
```

If you use an invalid schema, the server gives an exception error. You can turn off the validation of the beans.xml file by setting the `org.jboss.weld.xml.disableValidating=true` JVM property, which also prevents the error from being produced. If the beans.xml file specifies decorators or interceptors, a valid schema must be used, otherwise the decorators and interceptors are not correctly instantiated.

## Implicit bean archives

The CDI 1.2 implementation defines two different types of bean archives: explicit and implicit.

An explicit bean archive is an archive that contains a beans.xml file:

- with a version number of 1.1 (or later), and with the bean-discovery-mode of all
- with no version number
- that is an empty file

An implicit bean archive is any other archive, which contains one or more bean classes with a bean defining annotation as defined in the specification in Section 2.5.1, "Bean defining annotations", or one or more session beans. See the specification, Contexts and Dependency Injection for the Java EE platform.

When you update the schema to a CDI 1.2 implementation, to keep the bean archive as explicit the bean discovery mode must be set to all:

```
<beans xmlns="http://xmlns.jcp.org/xml/ns/javaee"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee  
http://xmlns.jcp.org/xml/ns/javaee/beans_1_1.xsd"  
bean-discovery-mode="all"  
version="1.1">
```

**Note:** An implicit bean archive discovers only beans that have a bean defining annotation.

This new type of bean archive can result in an archive that is not intended to be a CDI bean archive but it becomes an implicit bean archive in the CDI 1.2 implementation. To stop this behavior, you can add a beans.xml file with the bean discovery mode set to none, preventing the archive from being a bean archive. An alternative solution is to add the following property to the server.xml file for your Liberty server:

```
<cdi12 enableImplicitBeanArchives="false"/>
```

Setting this property to false prevents the archives without beans.xml files from becoming implicit bean archives.

Setting this property to false gives an improved performance at startup time.

# Administering Session Initiation Protocol (SIP) on Liberty

8.5.5.7

You can configure SIP on Liberty by adding and configuring elements in the `server.xml` file.

## Before you begin

Install the `sipServlet-1.1` feature in your Liberty server. For more information, see “Adding and removing Liberty features” on page 1587.

## About this task

8.5.5.7 This task describes how to manually configure SIP for Liberty in your `server.xml` file. Alternatively, you can configure SIP by using the developer tools, which automatically enable all configurations in the `server.xml` file. For more information, see [WebSphere Developer Tools > Developing > Developing SIP applications](#).

For information about the elements and attributes that you can use to configure SIP on Liberty, see the documentation for `SipServlet-1.1`.

## Procedure

1. In the `server.xml` file, configure the SIP container by adding a `sipContainer` element. For a full list of attributes and their descriptions, see `sipContainer` element.

```
<sipContainer invalidateSessionOnShutdown="true" msgArrivalTimeAttr="true" markInternalResponse="true"></sipContainer>
```

2. Configure the SIP stack by adding a `sipStack` element. You can configure behavior such as automatic responses, message information, and connection reuse.

For a full list of attributes and their descriptions, see `sipStack` element.

```
<sipStack hideMessageBody="true" hideMessageReqUri="true"
  auto100nInvite="false" auto4820nMergedRequests="true"
  forceConnectionReuse="false" acceptNonUtf8Bytes="true"
  pathMtu="1600" compactHeaders="API">
  <commaSeparatedHeaders>Comma separated headers</commaSeparatedHeaders>
  <hideMessageHeaders>iup</hideMessageHeaders>
  <sipQuotedParameters>Require</sipQuotedParameters>
</sipStack>
```

SIP timers provide a mechanism for session expiration. You can set values for the SIP timers that are different from default values that are specified in RFC 3261 by specifying the timer attributes on the `sipStack` element.

```
<sipStack timerT1="500" timerT2="4000" timerT4="5000" timerA="500" timerB="32000" timerD="32000"
  timerE="500" timerF="32000" timerG="500" timerH="32000" timerI="5000" timerJ="32000" timerK="5000"></sipStack>
```

3. Configure the SIP application router by adding a `sipApplicationRouter` element. When you configure a SIP application router, you can either use the default application router (DAR) or create a custom application router. The DAR component uses a configuration text file that is modeled as a Java properties file to define the order in which the application router sends SIP requests to applications.

If you do not configure an application router and are manually deploying your applications, applications are triggered in the order that the applications were deployed. If you deploy multiple applications through the `server.xml` file, you cannot define the application order.

- To use the DAR component with a DAR configuration file, specify the location of the DAR .properties file on the `sipDarConfiguration` attribute of the `sipApplicationRouter` element.

```
<sipApplicationRouter sipDarConfiguration="pathToDar.properties"></sipApplicationRouter>
```

- To use a custom application router, configure the router in the `server.xml` file:
  - a. Add the `bells-1.0` feature to the `server.xml` file.

```
<featureManager>
  <feature>bells-1.0</feature>
</featureManager>
```

For more information, see the documentation for bells-1.0.

- b. In the server.xml file, add your custom application router JAR file as a shared library and add the bell configuration for the javax.servlet.sip.ar.spi.SipApplicationRouterProvider service.

```
<library id="carLib" name="carLib" description="Custom App Router Library">
  <file name="pathToJar.jar"></file>
</library>
<bell libraryRef="carLib">
  <service>javax.servlet.sip.ar.spi.SipApplicationRouterProvider</service>
</bell>
```

For more information about shared libraries, see “Liberty: Shared libraries” on page 2254

- c. On the sipApplicationRouter element, set the carProvider attribute to the full name of the custom application router provider class.

```
<sipApplicationRouter carProvider="example.example"></sipApplicationRouter>
```

You can specify the error response code that the SIP container sends if no active servlet can be mapped to an incoming initial request by adding the sipNoRouteErrorCode attribute to the sipApplicationRouter element.

```
<sipApplicationRouter carProvider="example.example" sipNoRouteErrorCode="403"></sipApplicationRouter>
```

For a full list of attributes and their descriptions, see sipApplicationRouter element.

4. Configure the SIP endpoints by adding a sipEndpoint element. You can configure custom ports, hosts, and binding behavior. Any SIP endpoint that you configure overrides the default endpoint. For a full list of attributes and their descriptions, see sipEndpoint element.

```
<sipEndpoint host="localhost" sipTCPPort="5060" bindRetries="60" bindRetriesDelay="5000"></sipEndpoint>
```

**Note:** Transport Layer Security (TLS) is disabled by default. To enable TLS for your SIP container, enable and configure SSL communication for your Liberty server. For more information, see “Enabling SSL communication in Liberty” on page 1834.

5. Configure SIP performance by adding a sipTasksDispatcher element. You can configure the number of SIP tasks that can be run concurrently. A SIP application task is a sequence of application code that is serially executed on the SIP container on a single thread. For example, the application implementation of a SipServlet.doInvite() method or a SipTimerListener.timeout() method are each considered a single task if the application code that is called from these methods is executed serially on a managed Liberty thread that is provided by the container. The actual maximum number of concurrent SIP tasks is limited by the maximum number of managed Liberty threads.

For a full list of attributes and their descriptions, see sipTasksDispatcher element.

```
<sipContainer>
  <sipTasksDispatcher concurrentContainerTasks="15"/>
</sipContainer>
```

6. If you want to resolve SIP URIs by using Domain Name System (DNS) Naming Authority Pointer (NAPTR) records, configure a domain resolver.
  - a. Add and configure a domainResolver element. If you configure this element, SIP URIs are resolved through DNS into the IP address, port, and transport protocol of the next hop to contact.

**Note:** SIP does not support use of DNS procedures for a server to send a response to a back-up client if the primary client fails.

For a full list of attributes and their descriptions, see domainResolver element.

```
<domainResolver dnsAutoResolve="true">
  <dnsServers>dns.server.com</dnsServers>
</domainResolver>
```

- b. Configure your DNS server to work with the SIP container. The following example is a BIND db file for configuring RFC 3263 support on a DNS server.

```
; Copyright (C) 2004 Internet Systems Consortium, Inc. ("ISC")
; Copyright (C) 2001 Internet Software Consortium.
;
; Permission to use, copy, modify, and distribute this software for any
; purpose with or without fee is hereby granted, provided that the above
; copyright notice and this permission notice appear in all copies.
;
; THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
; REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
; AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
; INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
; LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
; OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
; PERFORMANCE OF THIS SOFTWARE.

; $Id: include.db,v 1.2.206.1 2004/03/06 10:22:13 marka Exp $

; Test $INCLUDE current domain name and origin semantics

example.com. 43200 IN SOA ns.example.com. email.example.com. ( 2003032001 10800 3600 604800 86400 )
;
example.com.          43200 IN NS      ns.example.com.
;
ns.example.com.      43200 IN A      10.0.0.20
sipserver1.example.com. 43200 IN A      10.0.0.21
sipserver2.example.com. 43200 IN A      10.0.0.22
sipserver3.example.com. 43200 IN A      10.0.0.23
;
router.example.com.  43200 IN CNAME sipserver3
;
sipserver1.example.com. 43200 IN AAAA    fec0:0:0:0:0:0:abcd
sipserver2.example.com. 43200 IN AAAA    fec0:0:0:0:0:0:abba
;
_sip_udp.example.com. 43200 IN SRV 2 0 5060 sipserver1.example.com.
_sip_udp.example.com. 43200 IN SRV 2 0 5060 sipserver2.example.com.
_sip_tcp.example.com. 43200 IN SRV 1 4 5060 sipserver1.example.com.
_sip_tcp.example.com. 43200 IN SRV 1 2 5060 sipserver2.example.com.
_sips_tcp.example.com. 43200 IN SRV 0 1 5061 sipserver1.example.com.
_sips_tcp.example.com. 43200 IN SRV 0 0 5061 sipserver2.example.com.
;
example.com. 43200 IN NAPTR 0 0 "s" "SIPS+D2T" "" _sips_tcp.example.com.
example.com. 43200 IN NAPTR 1 0 "s" "SIP+D2T" "" _sip_tcp.example.com.
example.com. 43200 IN NAPTR 2 0 "s" "SIP+D2U" "" _sip_udp.example.com.
```

**8.5.7** For information about performing DNS lookups in your SIP applications, see “Performing DNS lookups in Session Initiation Protocol (SIP) applications on the Liberty profile” on page 2131.

## Administering JavaMail on Liberty



**8.5.6**

You can configure JavaMail on Liberty by adding and configuring elements in the `server.xml` file.

### About this task

If you have an external mail server, you can use the JavaMail API to send and receive email on applications that are running on a Liberty server. The API allows applications to interact with the external mail server by providing common store and transport protocols, such as POP3, IMAP, and SMTP.

Liberty supports JavaMail 1.5. For more information about JavaMail 1.5, see the JavaMail API documentation.

For information about the elements and attributes that you can use to configure JavaMail on Liberty, see “JavaMail 1.5” on page 923.

## Procedure

1. In the `server.xml` file, add the `javaMail-1.5` feature. After you add the feature, you can call the JavaMail libraries in any application that runs on the server.  

```
<featureManager>
  <feature>javaMail-1.5</feature>
</featureManager>
```
2. Optional: If you want to create a `javax.mail.Session` object, add and configure a `mailSession` element. After the mail session is configured, the session is created and injected by using the Java Naming and Directory Interface (JNDI).

**Note:** If you use the standard JNDI context, `java:comp/env/mail/exampleMailSession`, configure the `jndiName` attribute as `jndiName="mail/exampleMailSession"`.

```
<mailSession mailSessionID="examplePop3MailSession"
  jndiName="ExampleApp/POP3Servlet/exampleMailSession"
  description="POP3 javax.mail.Session"
  storeProtocol="pop3"
  transportProtocol="smtp"
  host="exampleserver.com"
  user="iamaexample@example.com"
  password="example"
  from="smtp@testserver.com">
  <property name="mail.pop3.host" value="pop3.example.com" />
  <property name="mail.pop3.port" value="3110" />
</mailSession>
```

## Administering Liberty on z/OS

z/OS

On the z/OS platform you can start, stop, or modify Liberty by using MVS operator commands.

### Before you begin

Ensure that the following security profiles are set up as described in “Enabling z/OS authorized services in Liberty for z/OS” on page 1942.

- STARTED profiles for the server process, and the angel process
- SERVER profiles to allow access to authorized z/OS services

**Attention:** Each LPAR has one angel process. An angel started at service level 8.5.5.2 or later can coexist with other Liberty for z/OS servers that also use an angel at service level 8.5.5.2 or later. For multiple Liberty for z/OS servers that are running on the same LPAR with service levels before and after 8.5.5.2 that require an angel process, an angel at 8.5.5.2 or later will need to be started first to ensure proper operation of the angel process.

### About this task

This topic describes how to start, modify, and stop Liberty by using the MVS console. You can also start and stop the server from a shell, or use a shell to start the server as a started task, see “Starting and stopping a server from the command line” on page 1584.

A started task is JCL that is run immediately in response to an operator START command. Two JCL procedure templates (PROCs) are available in the `wlp/templates/zos/procs` directory. One template is for the server process, and the other is for the angel process:

- `bbgzsrv` for Liberty.

- bbgzangl for the angel process that is required for controlling access to system authorized services on the z/OS platform.

Administrators can copy the templates to a user location, and then customize them to start Liberty servers from the MVS console.

**Note:** Files in the /templates directories might be modified when product updates are applied. The examples section provides further information about the two PROC templates.

The target of an operator STOP command is a job or a started task.

After the JCL procedure templates are customized, they must be placed into the system procedure library concatenation. The name of the procedure member becomes the argument to the START command.

## Procedure

- To start a process, use the START (s) command for the appropriate proc:
  - START bbgzsrv to start the bbgzsrv proc for the server process
  - START bbgzangl to start the bbgzangl proc for the angel process
- To modify Liberty, use the MODIFY command. See the following topics:
  - “Liberty: Modify Commands on z/OS” on page 1734
  - “Liberty profile: Process types on z/OS” on page 1019
- To stop a process, use the STOP (p) command for the appropriate proc:
  - STOP bbgzsrv to stop the bbgzsrv proc
  - STOP bbgzangl to stop the bbgzangl proc

## Example

The following example shows the procedure template for the server process (bbgzsrv). This PROC is in a data set in the z/OS proclib concatenation.

```
//BBGZSRV PROC PARMS='defaultServer'
/*-----
/* INSTDIR - the path to the WebSphere Liberty install.
/*          This path is used to find the product code and is
/*          equivalent to the WLP_INSTALL_DIR environment variable
/*          in the Unix shell.
/* USERDIR - the path to the WebSphere Liberty user area.
/*          This path is used to store shared and server specific
/*          configuration information and is equivalent to the
/*          WLP_USER_DIR environment variable in the Unix shell.
/*-----
// SET INSTDIR='/u/MSTONE1/wlp'
// SET USERDIR='/u/MSTONE1/wlp/usr'
/*-----
/* Start the Liberty server
/*
/* WLPUDIR - PATH DD that points to Liberty's "user"
/*          directory. If the DD is not allocated, the user
/*          directory location defaults to the wlp/usr directory
/*          in the install tree.
/* STDOUT - Destination for stdout (System.out)
/* STDERR - Destination for stderr (System.err)
/* MSGLOG - Destination for messages.log (optional)
/* STDENV - Initial Unix environment - read by the system. The
/*          installation default and server specific server
/*          environment files will be merged into this environment
/*          before the JVM is launched.
/*-----
```

```

//STEP1 EXEC PGM=BPXBATSL,REGION=0M,
// PARM='PGM &INSTDIR./lib/native/zos/s390x/bbgzsrv &PARMS'
//WLPUDIR DD PATH='&USERDIR.'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
//*MSGLOG DD SYSOUT=*
//*STDENV DD PATH='/etc/system.env',PATHOPTS=(ORDONLY)
//*STDOUT DD PATH='&ROOT/std.out',
//* PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//* PATHMODE=SIRWXU
//*STDERR DD PATH='&ROOT/std.err',
//* PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//* PATHMODE=SIRWXU

```

### Notes:

- The launcher uses the STDENV DD as the initial environment, but this DD is optional. The initial environment to the process is defined in the PROC. It can point to any type of data set that LE supports, but the format must be compatible with what is expected. For example, EBCDIC, simple key=value with no expansion.
- A PATH DD that points to an existing directory (not a file) is allowed. If that DD is opened, the FILE stream that is returned is valid for fldata so the HFS path that is associated with the DD can be used. The PROC template defines a WLPUDIR PATH DD that represents the equivalent of WLP\_USER\_DIR.
- The WLP\_USER\_DIR is determined by the following logic:
  - If the WLPUDIR DD is defined, the associated path is used as WLP\_USER\_DIR
  - If WLPUDIR is not defined but WLP\_USER\_DIR is set in the initial environment (from STDENV), it is used
  - If WLPUDIR is not defined and WLP\_USER\_DIR is not set in the initial environment, the default value of \$WLP\_INSTALL\_DIR/usr is used
- The environment is determined by the following logic:
  - If the STDENV DD is defined, it is read by LE as the initial environment. If you want to set the \_BPX\_BATCH\_UMASK environment variable, it must be set here in the STDENV DD.
  - If \$WLP\_INSTALL\_DIR/etc/server.env exists and is readable, its key=value contents are read and set into the environment. The file can be in ASCII or EBCDIC. Comments start with a '#' and go to the end of the line. Values that contain white space can be placed in double quotation marks. Any environment entries that are specified in this file overrides entries from the initial environment
  - If \$WLP\_USER\_DIR/servers/{serverName}/server.env exists and is readable, its key=value contents are read and set into the environment. This file can also be in ASCII or EBCDIC and supports comments. Any entries that are specified here override entries from the initial environment and the etc/server.env.
  - Regardless of the user specified environment, the following entries are explicitly set: \_BPXK\_WLM\_PROPAGATE=NO, JAVA\_THREAD\_MODEL=HEAVY, and JAVA\_PROPAGATE=NO. If \_EDC\_PTHREAD\_YIELD is not set, it is set to -2.
- After the environment is set, the JAVA\_HOME is determined by the following logic:
  - If JAVA\_HOME is set in the environment, its location is used as JAVA\_HOME
  - If JAVA\_HOME is not set in the environment but \$WLP\_INSTALL\_DIR/./java64 exists, \$WLP\_INSTALL\_DIR/./java64 is used as JAVA\_HOME
  - If JAVA\_HOME is not set in the environment and \$WLP\_INSTALL\_DIR/./java64 does not exist, \$WLP\_INSTALL\_DIR/./java is used as JAVA\_HOME
- After JAVA\_HOME is determined, JVM command line options are determined by the following logic:
  - If \$WLP\_USER\_DIR/servers/{serverName}/jvm.options exists and is readable, its contents are read. The file can be in ASCII or EBCDIC and each line of the file should be a single java command line argument. Comments start at a '#' and go to the end of the line

- If \$WLP\_USER\_DIR/servers/{serverName}/jvm.options does not exist but \$WLP\_INSTALL\_DIR/etc/jvm.options exists and is readable, its contents are read. The file can be in ASCII or EBCDIC and must have one java command line argument per line. Comments are supported
- Regardless of the contents of any jvm.options, -Dfile.encoding=iso8859-1, -javaagent:\$WLP\_INSTALL\_DIR/lib/bootstrap-agent.jar, and -classpath \$WLP\_INSTALL\_DIR/lib/server-launcher.jar are on the command line
- If you want to pass arguments to the JVM, define the JAVA\_OPTS DD statement so that Java command line arguments are then read from this DD. The following example shows a sample input file:
 

```
-Xmx512m
-Xms256m
-Daaa.bbb.ccc=something.forsomeone
```
- When a Liberty server is started from a proc, the server validates that it is not running with a umask of 000. If it detects that the umask is 000, it overrides it with a value of 022.

The following example shows the command that you would use to start Liberty by using the sample bbgzsrv proc for a configured "defaultServer":

```
start bbgzsrv,parms='defaultServer'
```

The following example shows the procedure template for the angel process (bbgzangl):

```
//BBGZANGL PROC PARMS='',COLD=N
/*-----
// SET ROOT='/u/MSTONE1/wlp'
/*-----
/* Start the Liberty angel process
/*-----
//STEP1 EXEC PGM=BPXBATA2,REGION=0M,
// PARM='PGM &ROOT./lib/native/zos/s390x/bbgzangl COLD=&COLD &PARMS'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

## Liberty: Modify Commands on z/OS

z/OS

On the z/OS platform, you can modify Liberty by using MVS operator commands that are supported by a Liberty server process or that are supported by the Angel process.

### MODIFY commands that are supported by a Liberty server process

#### Trace enablement

The following example shows the **MODIFY** command to enable tracing for the specified Liberty server:

```
MODIFY [jobname.]identifier,LOGGING='<trace_specification>'
```

Substitute the value *trace\_specification* for a valid trace specification. For more information, see *Liberty: Logging and Trace*.

#### SVC dumps

To start an SVC dump, the server must be authorized with read access to the BBG.AUTHMOD.BBGZSAFM.ZOSDUMP resource profile in the SERVER class. The following example shows sample RACF commands for authorizing the server, where <userid> is the user ID assigned to the server:

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.ZOSDUMP UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSDUMP CLASS(SERVER) ACCESS(READ) ID(<USERID>)
SETR RACLIST(SERVER) GENERIC(SERVER) REFR
```

The following example shows the **MODIFY** command to request an SVC dump from the specified Liberty server:

```
MODIFY [jobname.]identifier,svcdump
```

### 8.5.5.2 Java heap dumps

The following example shows the **MODIFY** command to request a Java virtual machine (JVM) heap dump from the specified Liberty server:

```
MODIFY [jobname.]identifier,HEAPDUMP
```

### 8.5.5.2 Java core dumps

The following example shows the **MODIFY** command to request a JVM core dump from the specified Liberty server:

```
MODIFY [jobname.]identifier,JAVACORE
```

### 8.5.5.2 Server dumps

The following example shows the **MODIFY** command to request a server dump from the specified Liberty server:

```
MODIFY [jobname.]identifier,DUMP[,INCLUDE=<JAVA_DUMP_1>,<JAVA_DUMP_2>,...]
```

The **INCLUDE** parameter is optional. If the **INCLUDE** parameter is specified, any Java dumps that are listed on the **INCLUDE** parameter are requested and included in the server dump package. The following Java dump types are valid:

- THREAD for a Java core dump
- HEAP for a Java heap dump

## MODIFY commands that are supported by the Angel process

### Code version

The following example shows the **MODIFY** command to display the version of Angel code that is loaded:

```
MODIFY [jobname.]identifier,VERSION
```

### Enable or disable tracing

The following example shows the **MODIFY** command to enable or disable tracing for the Angel code:

```
MODIFY [jobname.]identifier,TRACE=[Y|N]
```

Select Y to enable tracing, or select N to disable tracing.

### Display servers

The following example shows the **MODIFY** command to display a list of servers that are currently connected to the Angel code:

```
MODIFY [jobname.]identifier,DISPLAY,SERVERS
```

## Liberty: APIs for z/OS command processing support

z/OS

The CommandHandler and ModifyResults application programming interfaces (APIs) are available for z/OS command processing support.

### com.ibm.ws.zos.command.processing.CommandHandler.java

The CommandHandler interface is the service that the command processing component looks for (by using the OSGi Whiteboard pattern). The command processing code will deliver any z/OS command string that matches its filter.

A z/OS modify command has the following format:

```
MODIFY <jobname.>identifier,command
```

The command value is matched against the **modify.filter.regex** property. The property value is treated as a regular expression.

For example, commands can be directed to the started job by issuing a z/OS modify command:

```
"MODIFY <jobname.>identifier,<cmdverb1>,<parm1>,<parm2>,( <moreInfo1>)
```

The **modify.filter.regex** property matches the value for the `<cmdverb1>,<parm1>,<parm2>,( <moreInfo1>)` command string. When the server receives the command, all currently registered CommandHandler's are matched, and the command is delivered according to the defined interface.

### **com.ibm.ws.zos.command.processing.ModifyResults.java**

The ModifyResults interface wraps the results of processing the command. It contains the command response messages and other information.

## **Enabling workload management for Liberty on z/OS**

z/OS

To enable access to z/OS native workload management (WLM) services for your applications running on Liberty, you use the zosWlm-1.0 feature with additional configuration.

### **About this task**

z/OS

For code examples, and for information about configuration syntax, classification rules, and the attributes of the `httpClassification` element, see “Liberty: WLM classification for z/OS” on page 1737.

### **Procedure**

- “Accessing authorized z/OS native WLM services on Liberty”
- “Accessing unauthorized z/OS native WLM services on Liberty” on page 1737

### **Accessing authorized z/OS native WLM services on Liberty:**

z/OS

To enable access to authorized z/OS native workload management (WLM) services, you use the Liberty zosWlm-1.0 feature, and define the security setup to permit the Authorized WLM Service (ZOSWLM).

### **Before you begin**

Start the Angel process using `<START bbgzang1>`. For more information, see “Administering Liberty on z/OS” on page 1731

z/OS

For code examples, and for information about configuration syntax, classification rules, and the attributes of the `httpClassification` element, see “Liberty: WLM classification for z/OS” on page 1737.

### **Procedure**

1. Enable the Liberty zosWlm-1.0 feature.
2. Define the security setup to permit the Authorized WLM Service (ZOSWLM).

### **Example**

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.ZOSWLM UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSWLM CLASS(SERVER) ACCESS(READ) ID(<USERID>)
```

The "subsystem name" used for classifying work requests is *BBGZSRV*, and it is specified on the WLM Connect Service `ConnectWorkMgr`.

The `collectionName` is supplied as the "COLLECTION" value on the `Classify` work (`__server_classify`). This example shows how the value used for the `collectionName` can be specified:

```
<zosWorkloadManager collectionName="AbcDef1234"/>
```

**Note:** The `collectionName` supports mixed case.

**Note:** The `collectionName` only uses the first 18 characters.

**Note:** If no value is specified, the value `/${wlp.server.name}` is used. This is the directory name of the server.

### Accessing unauthorized z/OS native WLM services on Liberty: z/OS

To enable access to unauthorized z/OS native WLM services, you use the Liberty `zosWlm-1.0` feature, and enable Liberty to use the native LE WLM services, such as `ConnectWorkMgr`, `createWorkUnit`, `deleteWorkUnit`, `extractWorkUnit`, `joinWorkUnit` and `leaveWorkUnit`.

#### Before you begin

z/OS For code examples, and for information about configuration syntax, classification rules, and the attributes of the `httpClassification` element, see "Liberty: WLM classification for z/OS."

#### Procedure

1. Enable the Liberty `zosWlm-1.0` feature.
2. Define a security profile for the FACILITY class and profile "BPX.WLMSEVER" that allows the user associated with the server READ access. This enables the Liberty server to use the native LE WLM services, such as `ConnectWorkMgr`, `createWorkUnit`, `deleteWorkUnit`, `extractWorkUnit`, `joinWorkUnit` and `leaveWorkUnit`.

#### Example

The "subsystem name" used for classifying work requests is *BBGZSRV*, and it is specified on the WLM Connect Service `ConnectWorkMgr`.

The `collectionName` is supplied as the "COLLECTION" value on the `Classify` work (`__server_classify`). This example shows how the value used for the `collectionName` can be specified:

```
<zosWorkloadManager collectionName="AbcDef1234"/>
```

**Note:** The `collectionName` supports mixed case.

**Note:** The `collectionName` only uses the first 18 characters.

**Note:** If no value is specified, the value `/${wlp.server.name}` is used. This is the directory name of the server.

### Liberty: WLM classification for z/OS: z/OS

Syntax and support notes about Liberty for z/OS workload management (WLM) feature.

A WLM enclave is associated with the thread that the request is dispatched on. It is also associated with a WLM Service Class. A WLM Service Class is assigned to the WLM enclave by WLM, based on rules

that you define in the WLM configuration. The WLM Service Class indicates the WLM goals for each class of client work, for example, 95% complete in 1 second or less. The WLM Service Class also indicates the importance of the goals relative to other work on the system. WLM uses information that is provided by the Liberty server during classification to assign a WLM Service Class. The following three properties help WLM to classify the work:

**Subsystem Type**

For WebSphere, Subsystem Type is CB.

**Collection Name**

Name of the server that is running the work. You can create WLM classification rules that are based on the server that is running the work.

**Transaction Class**

Name that is determined from classification of the work within the Liberty code. Transaction Class is based on the Liberty configuration that you provide for the request that is being dispatched. You can assign different Transaction Classes to different applications within the same server, and thus different WLM Service Classes.

Syntax for configuration in the server.xml file:

```
<featureManager>
  <feature>zosWlm-1.0</feature>
</featureManager>

<wlmClassification>
  <httpClassification transactionClass="CLASS001" host="127.0.0.1" port="9080" method="GET"
    resource="/testResource" />
</wlmClassification>
```

Table 123. Default Values

Attributes	Default values
transactionClass=""	Empty string
host="*"	Wildcard
port="*"	Wildcard
method="*"	Wildcard
resource="*"	Wildcard

**Important:**

- All attributes of <httpClassification ... /> are optional.
- If you turn on WLM, but do not specify a minimum of one rule, WLM is active but no enclaves are created.
- Classification rules have a top-down ordering, that is, each rule takes precedence over all rules below it.
- Transaction Classes can be mixed case.
- Ports can be specified as ranges. For example, port="9080-9085".
- Ports and methods can be specified as a comma-separated list. For example, port="9043,9080" or method="GET,PUT".
- Resources can be specified by using wildcards. One asterisk represents any number of characters, and is used as a wildcard for the string between two path separator (/) characters. Two consecutive asterisks represent any number of characters that include the path separator. Double asterisks cannot appear with other characters within a pair of path separators.
  - resource="/test\*/\*" matches /testaa/bb.html, but does not match /testaa/bb/cc.html
  - resource="\*.html" matches /aaa.html but does not match/aaa/bbb.html

- resource="/go/set\*/\*\*/archive.jsp" matches /go/seta/bb/2/archive.jsp, /go/setaa/bb/2/archive.jsp, and /go/set/archive.jsp
- The default, if resource= is not specified, matches ALL strings, which is equivalent to resource="\*\*/\*", which matches /aaa, /aaa/bbb, and /aaa/bbb/cc.html

Example configuration:

```
<wlmClassification>
  <httpClassification transactionClass="CLASS004" resource="/res2"/>
  <httpClassification transactionClass="CLASS003" resource="/res1"/>
  <httpClassification transactionClass="CLASS002" port="9043" />
  <httpClassification transactionClass="CLASS001" />
</wlmClassification>
```

#### Notes:

- Rules 1 and 2 catch all incoming requests to their respective resources
- Rule 3 catches any incoming request not to either listed resource but on port 9043
- Rule 4 is a "catch-all" rule, which matches any request that comes in that was not matched by Rule 1, Rule 2, or Rule 3

## Enabling syncToOSthread for applications



To enable **syncToOSthread** on Liberty, you use the **appSecurity-1.0** and **zosSecurity-1.0** features with additional configuration.

### Before you begin

Enabling **syncToOSthread** support requires the **appSecurity-1.0** and **zosSecurity-1.0** features. You must also define the **syncToOSthread** configuration element. In addition, you must use the SAF registry for authentication, and authorized SAF services must be available.

Because **syncToOSthread** support requires authorized SAF services, the angel process must be up and running and the server must be connected to it. For more information about the angel process, see “Liberty profile: Process types on z/OS” on page 1019.

### Procedure

1. Configure the application to use **syncToOSthread** by adding the following **env-entry** to the application's deployment descriptor:

```
<env-entry>
  <env-entry-name>com.ibm.websphere.security.SyncToOSthread</env-entry-name>
  <env-entry-type>java.lang.Boolean</env-entry-type>
  <env-entry-value>true</env-entry-value>
</env-entry>
```

2. Configure the server to enable **syncToOSthread** for applications by adding the **appSecurity-1.0** and **zosSecurity-1.0** features, and defining the **syncToOSthread** configuration element with attribute appEnabled="true". Additionally, ensure the SAF registry must be used for authentication:

```
<featureManager>
  <feature>appSecurity-1.0</feature>
  <feature>zosSecurity-1.0</feature>
</featureManager>

<safRegistry id="saf" />
<syncToOSthread appEnabled="true" />
```

3. Grant the server permission to perform **syncToOSthread** operations by configuring your SAF product with either of the following profiles:

- Grant the userid of the server CONTROL access to the BBG.SYNC.<profilePrefix> profile in the FACILITY class. This allows the server to sync any RunAs identity with the OS identity:  
`PERMIT BBG.SYNC.<profilePrefix> ID(<serverUserId>) ACCESS(CONTROL) CLASS(FACILITY)`
- Grant the userid of the server READ access to the BBG.SYNC.<profilePrefix> profile in the FACILITY class. Additionally, grant the userid of the server READ access to one or more BBG.SYNC.<runAsUserId> profiles in the SURROGATE class, one for each RunAs identity to be synchronized with the OS identity:  
`PERMIT BBG.SYNC.<profilePrefix> ID(<serverUserId>) ACCESS(READ) CLASS(FACILITY)`  
`PERMIT BBG.SYNC.<runAsUserId> ID(<serverUserId>) ACCESS(READ) CLASS(SURROGAT)`

**Note:** The <profilePrefix> is by default “BBGZDFLT” and can be configured by using the <safCredentials profilePrefix="xx"> element in your configuration file.

For more information about **syncTo0SThread**, see Java thread identity and an operating system thread identity

## Enabling syncTo0SThread for J2C connections

z/OS

8.5.0.2

To enable **syncTo0SThread** for J2C connections on Liberty, you use the **appSecurity-1.0** and **zosSecurity-1.0** features with additional configuration.

### Before you begin

Enabling **syncTo0SThread** support for J2C connections requires the **appSecurity-1.0** and **zosSecurity-1.0** features. You must also define the **syncTo0SThread** configuration element. In addition, you must use the SAF registry for authentication, and authorized SAF services must be available.

Because **syncTo0SThread** support requires authorized SAF services the angel process must be up and running and the server must be connected to it. For more information about the angel process, see “Liberty profile: Process types on z/OS” on page 1019.

### Procedure

1. Configure the server to enable **syncTo0SThread** for J2C connections by adding the **appSecurity-1.0** and **zosSecurity-1.0** features and defining the **syncTo0SThread** configuration element with attribute `j2cEnabled="true"`. Additionally, ensure the SAF registry must be used for authentication:

```
<featureManager>
  <feature>appSecurity-1.0</feature>
  <feature>zosSecurity-1.0</feature>
</featureManager>

<safRegistry id="saf" />
<syncTo0SThread j2cEnabled="true" />
```

#### Note:

- For connections that use a resource that specifies `res-auth=container`, setting `j2cEnabled=true` enables **syncTo0SThread** for type-2 J2C connections. Enablement of **syncTo0SThread** synchronizes the Java RunAs identity with the OS identity during the establishment of the connection. The connection is thereby associated with the OS identity and is assigned the same permissions and privileges as the OS identity.
  - Do not specify a JAAS alias for the data source if you wish to use **syncTo0SThread**. The JAAS alias, if defined, will override the OS identity.
2. Grant the server permission to perform **syncTo0SThread** operations by configuring your SAF product with either of the following profiles:
    - Grant the userid of the server CONTROL access to the BBG.SYNC.<profilePrefix> profile in the FACILITY class. This allows the server to sync any RunAs identity with the OS identity:

```
PERMIT BBG.SYNC.<profilePrefix> ID(<serverUserId>) ACCESS(CONTROL) CLASS(FACILITY)
```

- Grant the userid of the server READ access to the BBG.SYNC.<profilePrefix> profile in the FACILITY class. Additionally, grant the userid of the server READ access to one or more BBG.SYNC.<runAsUserId> profiles in the SURROGATE class, one for each RunAs identity to be synchronized with the OS identity:

```
PERMIT BBG.SYNC.<profilePrefix> ID(<serverUserId>) ACCESS(READ) CLASS(FACILITY)
PERMIT BBG.SYNC.<runAsUserId> ID(<serverUserId>) ACCESS(READ) CLASS(SURROGAT)
```

**Note:** The <profilePrefix> is by default “BBGZDFLT” and can be configured by using the <safCredentials profilePrefix="xx"> in your configuration file.

For more information about **syncToOSThread**, see Java thread identity and an operating system thread identity

---

## Administering Liberty using Admin Center



8.5.5.2

You can use WebSphere Liberty Administrative Center ("Admin Center") to administer Liberty servers and applications and other resources from a web browser on a smartphone, tablet, or computer.

### About this task

Use the Admin Center with a Liberty server or Liberty Core installation. An installation of the WebSphere Application Server full profile is not required.

Admin Center offers the ability to start, stop, and view details about Liberty servers and applications. It also offers the ability to edit server configuration files, to view bookmarked information, to add tools, to monitor server resources, and to deploy server packages on hosts within a collective. Advantages of the Admin Center design include:

- A user interface with a mobile look-and-feel for web browsers on a smartphone or tablet
- Support for multiple lightweight, task-oriented tools
- A toolbox that you can customize by selecting tools from a catalog, specifying bookmarks, or specifying user preferences

 **Watch:** The Touring Admin Center video shows the user interface and briefly describes Admin Center features. [Transcript]

### Procedure

1. Set up Admin Center.
  - Install Liberty with Admin Center.
  - Configure the server.xml file to enable Admin Center and secure login.
  - If the server is not running, start the server.
2. Log in to Admin Center.
  - Point a web browser at Admin Center.
  - On the Welcome page, specify an authorized user name and password to log in.
3. Use the Toolbox.
  - Select a tool or bookmark.
  - Add a tool.
  - Remove a tool.
  - Add or remove a bookmark.
  -  Rearrange tool and bookmark icons.
  - Filter toolbox contents.
  - Edit user preferences such as text direction.

- **8.5.5.6** Uninstall an Admin Center tool.
4. **8.5.5.7** Use the Server Config tool to view and edit server configuration files in the Liberty topology.
    - Enable editing of files to change `server.xml` or any other files in the server configuration directory.
    - View or edit a configuration file in the Server Config tool.
    - Customize a default setting for Design or Source mode.
  5. Use the Explore tool to explore and manage resources in the Liberty topology.
    - View a summary of all resources on the Explore tool Dashboard.
    - View a summary of all applications, clusters, servers, or hosts.
    - View details about a resource.
    - **8.5.5.4** View details about all servers on a Liberty runtime.
    - Start, stop, or restart a resource.
    - Deploy a server package on a host from the Explore tool.
    - **8.5.5.5** Search for resources.
  6. **8.5.5.5** Optional: View charts of server or application metrics in the Monitor view of the Explore tool.
    - Open the Monitor view on a server or application.
    - Show or hide charts.
    - Show or hide chart legends.
    - **8.5.5.6** View chart data in a table.
  7. **8.5.5.5** Optional: Set and view administrative metadata for server, cluster, or application resources in the Explore tool.
    - **8.5.5.6** Set and view administrative metadata for resources in the Tags and Metadata dialog of the Explore tool.
    - View administrative metadata defined in an `admin-metadata.xml` file in the Explore tool.
  8. **8.5.5.7** Optional: Enable maintenance mode for a server or host in the Explore tool.
  9. Optional: Use the Deploy tool to install Liberty server package (archive) files on hosts within a collective.
  10. Optional: After using the Deploy tool, use the Background Tasks page to check the status of Deploy Installation tasks.
  11. After completing work in Admin Center, log out.

## Setting up Admin Center



**8.5.5.2**

Admin Center is a web user interface that runs on Liberty V8.5.5.2 and later servers. After installing Liberty and creating a server, configure the `server.xml` file.

### Before you begin

Install WebSphere Application Server Liberty with Liberty Administrative Center ("Admin Center"). The Installing Liberty Repository assets topic lists the ways to install assets such as Admin Center. The quickest way to install Admin Center is to run the **installUtility** command or the **featureManager** command:

1. If you have not done so already, install WebSphere Application Server Liberty V8.5.5.2 or later.

**Restriction:** Ensure that you use a Java virtual machine (JVM) that supports Liberty products and Secure Sockets Layer (SSL). Do not use an IBM JVM available with a WebSphere Application Server traditional product, such as Network Deployment, for your Liberty installation with Admin Center. By default, the IBM JVM available with a traditional product points to security classes that are available only with a traditional product, and not to security classes needed by Admin Center. Using an IBM JVM available with a traditional product can cause Admin Center to not display in a browser.

2. Open a command window at the main directory of the Liberty installation. For example, open a command window at `c:\wlp`.
3. Run a command to install the `adminCenter-1.0` feature.

**8.5.5.6** For Version 8.5.5.6 or later, run the **installUtility** command:

```
bin/installUtility install adminCenter-1.0
```

For Version 8.5.5.5 or earlier, run the **featureManager** command:

```
bin/featureManager install adminCenter-1.0 --when-file-exists=ignore
```

4. For the Liberty Developers edition, run a command to install the `collectiveController-1.0` feature.

**8.5.5.6** For Version 8.5.5.6 or later, run the **installUtility** command:

```
bin/installUtility install collectiveController-1.0
```

For Version 8.5.5.5 or earlier, run the **featureManager** command:

```
bin/featureManager install collectiveController-1.0 --when-file-exists=ignore
```

This step applies only to the Developers edition and not to the Network Deployment, z/OS or Core editions of Liberty. Optionally, you can install the `collectiveController-1.0` feature before installing the `adminCenter-1.0` feature.

For more information, go to the WASdev website, select the **Downloads** tab, and search the Liberty repository for the Admin Center asset.

To install Admin Center on hosts that cannot access the internet-based Liberty repository, first install Liberty and the Admin Center feature on a host that can access the internet. Then transfer the installation to the target hosts. For information about packaging Liberty servers and runtimes for deployment to other hosts, see Packaging a Liberty server by using developer tools and Packaging a Liberty server from the command line.

## About this task

You can set up Admin Center on stand-alone servers and on collective controllers. This topic focuses on setting up a stand-alone Liberty server.

To enable Admin Center on a collective controller, see Configuring a Liberty collective and the example in Deploying resources with Admin Center. Ensure the `server.xml` file of the collective controller includes `<feature>adminCenter-1.0</feature>` in the feature manager configuration and sets a host value in the `httpEndpoint` element, such as `host="*"` so all hosts can access the collective controller.

## Procedure

1. If your Liberty installation does not have a server, create a Liberty server.

For example, in a command window at the `wlp/bin` directory, create a server named `myServer`.

```
server create myServer
```

The example command adds server files to the `wlp/usr/servers/myServer` directory.

2. Open an editor on the `server.xml` file of the Liberty server, and configure the server for Admin Center.

- a. Add the `adminCenter-1.0` feature to the feature manager.

```
<featureManager>
  <feature>adminCenter-1.0</feature>
</featureManager>
```

For more timely updates to server and application status in the Explore tool, also add the `websocket-1.1` or `websocket-1.0` feature to the server configuration.

```
<featureManager>
  <feature>adminCenter-1.0</feature>
  <feature>websocket-1.1</feature>
</featureManager>
```

WebSocket provides a live view of the topology regardless of size. Without the WebSocket feature, Admin Center periodically and frequently polls for changes.

- b. Add one or more users to configure a secure login. For example:

```
<quickStartSecurity userName="admin" userPassword="adminpwd" />
```

If user names or passwords include non-English characters, create the `jvm.options` file for the server and define the default client encoding as UTF-8:

```
-Ddefault.client.encoding=UTF-8
```

For information about the `jvm.options` file, see “Customizing the Liberty environment” on page 1565.

- c. To protect keystore files that have server authentication credentials, define a keystore and assign it a password.

```
<keyStore id="defaultKeyStore" password="Liberty" />
```

For an example `server.xml` file that defines an Administrator and a non-Administrator and that defines a keystore, see the Example in this topic. For information about defining multiple administrative users, see “Setting up BasicRegistry and role mapping on Liberty” on page 1832.

- d. To access Admin Center from a smartphone, tablet, or remote computer, ensure that the `server.xml` file sets the host attribute of the `httpEndpoint` element to \* (asterisk) or to a defined host name. By default, the host attribute is set to `localhost`.

```
<httpEndpoint id="defaultHttpEndpoint"
  host="*"
  httpPort="9080"
  httpsPort="9443" />
```

- e. Save your changes to the `server.xml` file.

If you defined the default client encoding as UTF-8 for non-English characters in the `jvm.options` file and the user registry is in `quickStartSecurity` or `basicRegistry` elements, which store user names and passwords in the `server.xml` file, then save the `server.xml` file in UTF-8 encoding.

3. If the server is not running, start the server.

For example, in a command window at the `wlp/bin` directory, enter a **run** or **start** command.

```
server run myServer
```

Look for server messages that show the `adminCenter` web application is running. After Admin Center is running, you can point a web browser at the application and log in. See “Logging in to Admin Center” on page 1745.

 **Watch:** The Setting up Admin Center video demonstrates the procedure. [Transcript]

## Example: server.xml file that defines two authorized users

```
<server description="new server">

  <!-- Enable features -->
  <featureManager>
    <feature>adminCenter-1.0</feature>
  </featureManager>

  <!-- Define the host name for use by the collective.
  If the host name needs to be changed, the server should be
  removed from the collective and re-joined. -->
  <variable name="defaultHostName" value="localhost" />

  <!-- Define an Administrator and non-Administrator -->
  <basicRegistry id="basic">
    <user name="admin" password="adminpwd" />
    <user name="nonadmin" password="nonadminpwd" />
  </basicRegistry>

  <!-- Assign 'admin' to Administrator -->
  <administrator-role>
    <user>admin</user>
  </administrator-role>
```

```
<keyStore id="defaultKeyStore" password="Liberty" />

<httpEndpoint id="defaultHttpEndpoint"
  host="*"
  httpPort="9080"
  httpsPort="9443" />

</server>
```

## Logging in to Admin Center



After the Admin Center web application starts, you can point a web browser at Admin Center and log in. After logging in, the first page shown is the Toolbox.

### Before you begin

Ensure that you have a browser that supports Admin Center.

- For browsing the Admin Center on a computer: Firefox ESR 24, Firefox 29, Chrome 35, Safari 7, or Internet Explorer 11 browser (for best experience, use Chrome or Firefox browser)
- For browsing the Admin Center on an iPhone or iPad: Safari browser on iOS 6.x or 7.x
- For browsing the Admin Center on an Android mobile device: Chrome browser on Android 4.2 or 4.3

### Procedure

1. Point a web browser at Admin Center.

```
https://host_name:port_number/adminCenter/
```

For *host\_name*, specify the IP address or domain name server (DNS) host name of the computer on which the Liberty server is running. Specify localhost only if the browser is running on the same computer as the server.

For *port\_number*, specify the httpsPort value in the server.xml file. For example:

```
https://localhost:9443/adminCenter/
```

```
https://myhost.xyz.com:9443/adminCenter/
```

```
https://9.65.234.567:9443/adminCenter/
```

2. If your browser prompts you to confirm that the connection is trusted, specify an exception or otherwise enable the connection to continue to Admin Center.
3. Log in to Admin Center.

When you configured the server.xml file of the server to enable Admin Center, you defined one or more user names and passwords authorized to access the Admin Center. To log in to Admin Center, specify an authorized user name and password.

For example, specify the user name admin and the password adminpwd.

### What to do next

When you first access the Toolbox, it has the Server Config and Explore tools and a bookmark to WASdev.net. The Toolbox also has the Deploy tool if Admin Center is run on a collective controller. The Deploy tool is not available if Admin Center is run on a stand-alone server.



To add or remove tools and bookmarks, select  and use the Tool Catalog to customize your user-specific Toolbox.

**8.5.5.4** To view a tool, select its Toolbox icon or directly launch the tool using the URL that is shown in the browser when viewing the tool. For example, to directly launch the Explore tool, use a URL such as `https://localhost:9443/adminCenter/#explore`.

Later, to log out of Admin Center, select  > **Log out *user\_name***.

## Customizing the Toolbox

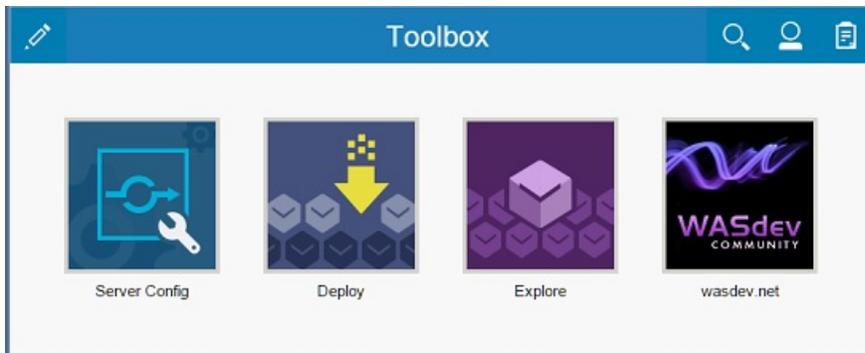


When you first log in to Admin Center, the Toolbox contains the Server Config and Explore tools and a bookmark to WASdev.net. The Toolbox also has the Deploy tool if the server hosting Admin Center is a collective controller. You can edit the Toolbox contents by adding tools from the Tool Catalog or by adding bookmarks. A *tool* is a web application that performs a particular task and is typically provided by the product. A *bookmark* is a user-added link to any site. You can further customize your Toolbox by rearranging icons, filtering Toolbox contents, or editing preferences.

### About this task

Select tools, bookmarks, and menu choices in the Toolbox to use Admin Center. The Toolbox offers the following options:

- Select a tool or bookmark.
- Add a tool.
- Remove a tool.
- Add or remove a bookmark.
- Rearrange tool and bookmark icons.
- Filter toolbox contents.
- Edit user preferences such as text direction.
- **8.5.5.6** Uninstall an Admin Center tool.



## Procedure

- To work with an existing tool or to open a browser on a bookmarked URL, select the icon for the tool or bookmark.
- Add tools.
  1. Select  >  > **Add Tool**.
  2. Select  on the tool to add.
  3. Confirm that you want to add the tool.
  4. Select  to return to the Toolbox.

**8.5.5.4** After you add a tool, use the Toolbox to first launch the tool. To directly launch the tool at a later time, you can use the URL that is shown in the browser when viewing the tool.
- Remove tools.
  1. Select .
  2. Select  on the tool to remove.
  3. Confirm that you want to remove the tool.
  4. Select  to return to the Toolbox.
- Add or remove bookmarks.
  1. Select  >  > **Add Bookmark**.
  2. Enter the bookmark name and URL, and then select **Add** to add the bookmark to your Toolbox. To later remove the bookmark, select the bookmark and then .
  3. Select  to return to the Toolbox.
- **8.5.5.4** Rearrange tool and bookmark icons.
  1. Select .
  2. Drag and drop the icons into the order that you prefer.
  3. Select  to return to the Toolbox.
- Filter toolbox contents.
  1. Select .
  2. Type the tool or bookmark name in the text field. Filtered search results are shown if the characters typed match the names of Toolbox contents.
  3. After searching, select  to close the text field.
- Edit your preferences.

1. Select  > **Preferences**.
2. For **Enable bidirectional support**, specify whether text displays left to right, the default, or displays right to left. Select **Contextual** for the first typed character to determine the direction. When the first character is in a language such as Arabic or Hebrew, control orientation and typing direction become right to left, with right alignment for text.
3. Select  to return to the Toolbox.

- **8.5.5.6** Uninstall an Admin Center tool.

By default, the Toolbox contains Admin Center tools such as the Explore tool and, if the server hosting Admin Center is a collective controller, the Deploy tool. You can use the feature manager to uninstall Admin Center tools to fully customize your Toolbox. Run the **uninstall** command for featureManager. For example, if you use DevOps you might want to uninstall the Deploy tool. To do so, run:

```
wlp/bin/featureManager uninstall com.ibm.websphere.appserver.adminCenter.tool.deploy-1.0
```

Admin Center tools use the `com.ibm.websphere.appserver.adminCenter.tool.*` naming format:

- `com.ibm.websphere.appserver.adminCenter.tool.explore-1.0.mf`
- `com.ibm.websphere.appserver.adminCenter.tool.deploy-1.0`

## What to do next

Your selections are saved for the user name that was specified when logging in. If you later log in under the same user name, the Toolbox shows the same tool, bookmark, and preference selections as when you last logged out. If you log in under a different user name, the Toolbox shows the selections for that other user name.

## Editing server configuration files in Admin Center

**8.5.5.7**

You can use the Server Config tool to view and edit server configuration files in the Liberty topology. The Server Config tool displays configuration files such as a `server.xml` file in two modes. The Design mode displays the content of configuration files using graphical controls with inline documentation. The Source mode provides direct access to the file text and has content assist capabilities. You can customize the modes, for example, to add or remove parameter descriptions on the Design mode or to add or remove line numbers on the Source mode. Before you can edit files, you must add a `remoteFileAccess` element to the server configuration file; otherwise, files are shown in read-only mode.

**8.5.5.8**

### About this task

 **Watch:** The Getting started with the Server Configuration Tool for WebSphere Liberty video shows how to enable and use the tool.

### Procedure

1. Enable editing of files in the server configuration directory.

- a. Open an editor on the server configuration file.

The configuration file for a server typically has a path name such as `wlp/usr/servers/server_name/server.xml`.

- b. Add the following `remoteFileAccess` element to the server configuration file.

```
<remoteFileAccess>
  <writeDir>${server.config.dir}</writeDir>
</remoteFileAccess>
```

- c. Save the file changes.

Server configuration files such as the `server.xml` and any included files no longer are read-only in the Server Config tool. You can change element and parameter settings, and otherwise edit the files.

2. View or edit a configuration file in the Server Config tool.

- a. From the Toolbox, select .
- b. If Admin Center is run on a collective controller, select the server that has the configuration file you want to view or edit.
- c. After a file is open for editing, you can switch between **Design** and **Source** modes.

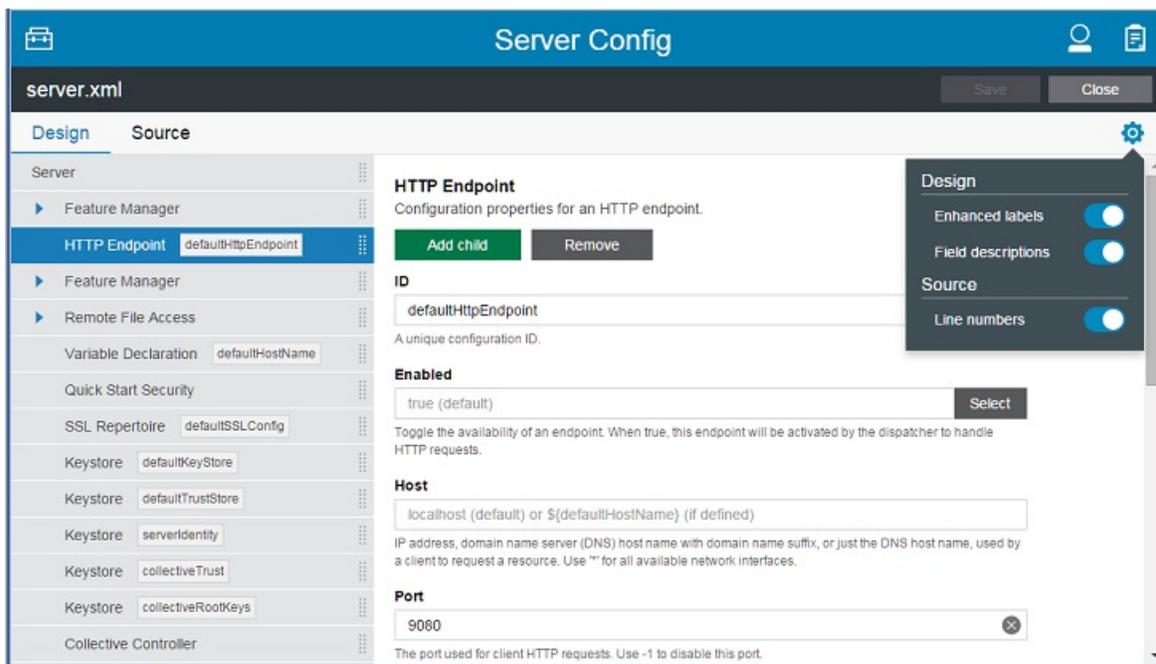
In the Design mode, select elements in the configuration to see enabled features and parameter settings.

In the Source mode, hover on elements and parameters to view their documentation. You can press Ctrl+Space to use content assist, which helps you add new elements, parameters, and values.

- d. After you finish working with a file, select **Save** to save the file changes and then **Close** to return to the main page of the tool. To discard file changes, select **Close** and then confirm to not save the changes.
3. Optional: Customize the default settings for Design or Source mode.

By default, the Design mode uses enhanced labels for file elements. Enhanced labels display element names such as featureManager as Feature Manager. Also, the Design mode displays parameter descriptions by default. The Source mode displays line numbers by default. To change a default setting:

- a. Select .
- b. Enable or disable one or more default settings.
- c. Select **Close**.



## What to do next

To return to the Toolbox, select .

## Exploring and managing resources with Admin Center



You can use the Explore tool to view and manage resources in the Liberty topology.

## About this task

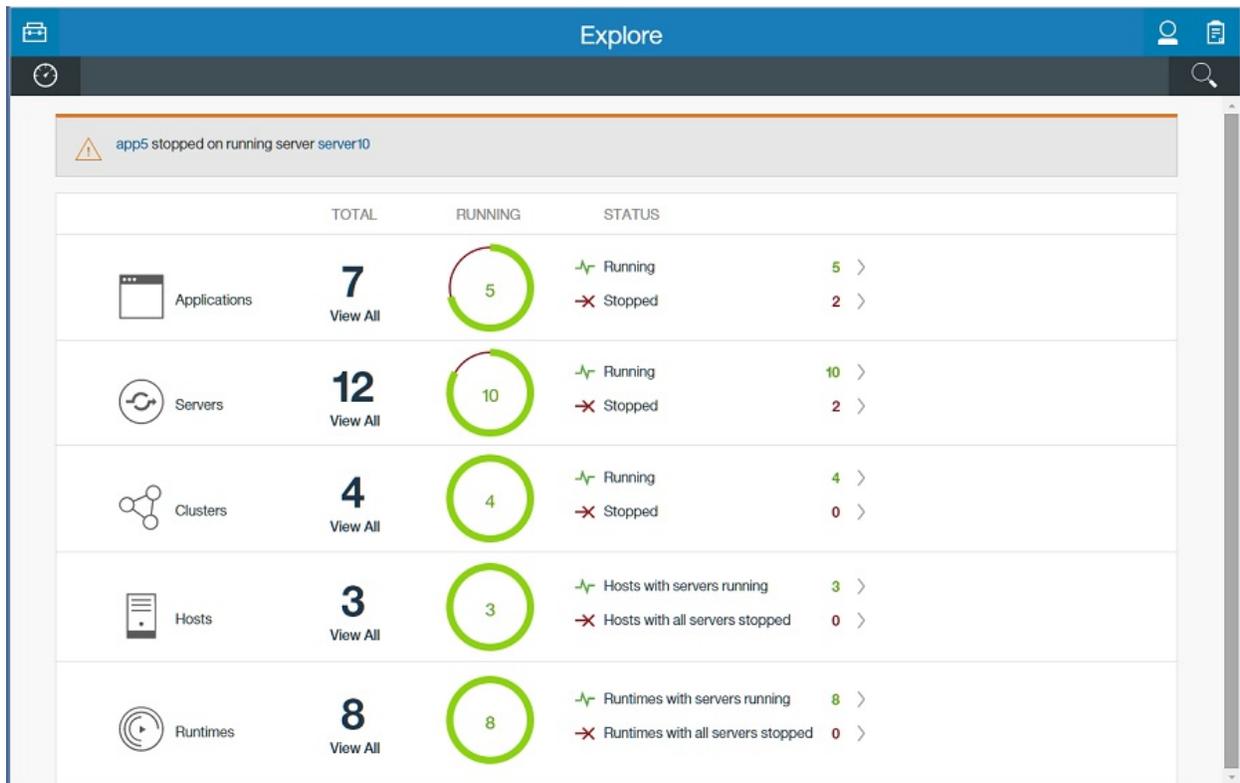
The Explore tool offers the following options to work with application, server, cluster, host, and runtime resources:

- View a summary of all resources on the Dashboard.
- View a summary of all applications, servers, clusters, hosts, or runtimes.
- View details about a resource.
- [8.5.5.4](#) View details about all servers on a Liberty runtime.
- Start, stop, or restart a resource.
- Deploy a server package on a host from the Explore tool.
- [8.5.5.5](#) Search for resources.

## Procedure

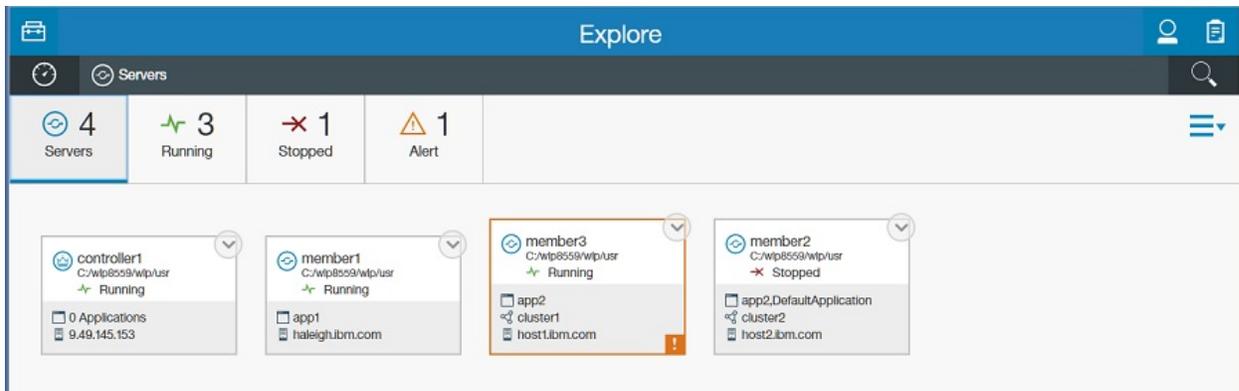
- View a summary of all resources on the Explore tool Dashboard.

From the Toolbox, select . The Explore page, or "Dashboard," shows the number of applications, servers, clusters, hosts, and runtimes that Admin Center is managing. The Dashboard also shows the number of resources that are running, stopped, or in an unknown state. If an alert condition is met, the alert is shown on the Dashboard with a link to the appropriate resource page. The resource name, total, and status also have links to the appropriate resource pages.



- View a summary of all applications, servers, clusters, hosts, or runtimes.

From the Dashboard, select a link on the **Applications**, **Servers**, **Clusters**, **Hosts**, or **Runtimes** panel. For example, to see a summary of all servers, select the **View All** link on the **Servers** panel. The state of all servers is shown. Whether a server is a collective controller or stand-alone server is also shown.



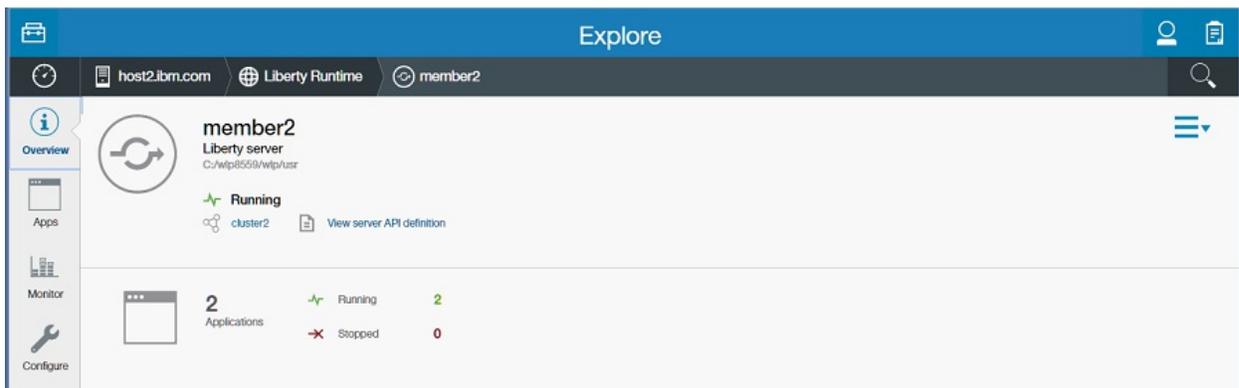
If an alert condition is met, an exclamation mark  is shown on the resource card. Select  for details on the alert condition.

To filter the view, select an icon that shows the number of resources in a specific state. For example, select the **1 Alert** icon to display the one server with an alert condition.

For more timely updates to server and application status, add the websocket-1.1 or websocket-1.0 feature to the server configuration for your servers that use the adminCenter-1.0 feature.

- View details about a resource.

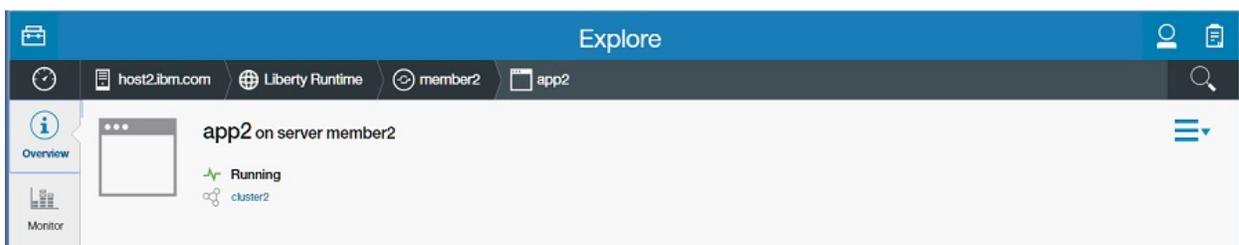
From the Explore page, select a link on the **Applications**, **Servers**, **Clusters**, **Hosts**, or **Runtimes** panel and then a specific resource. For example, to see details about a server, select a link on the **Servers** panel and then one of the servers.



If an alert condition is met, the alert is described with a link to the appropriate resource page.

**8.5.5.9** If the apiDiscovery-1.0 feature is in the configuration file for a server, the  icon with the **View server API definition** link is shown in details about the server. When the server is stopped, the **View server API definition** link is unavailable. For information about the apiDiscovery-1.0 feature, see “Discovering REST API documentation on a Liberty server” on page 2260.

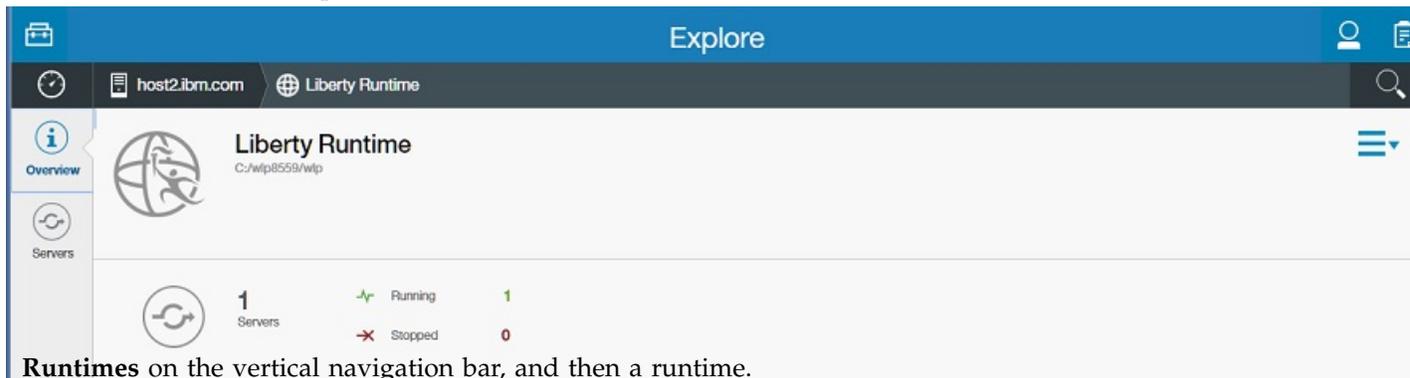
For resources on Liberty servers, select a resource to see more details. For example, select **Apps** and then an application to display details about the application on one of the servers. From the application details page you also can access the Monitor view for each application.



- 8.5.5.4 View details about all servers on a Liberty runtime.

From the Dashboard:

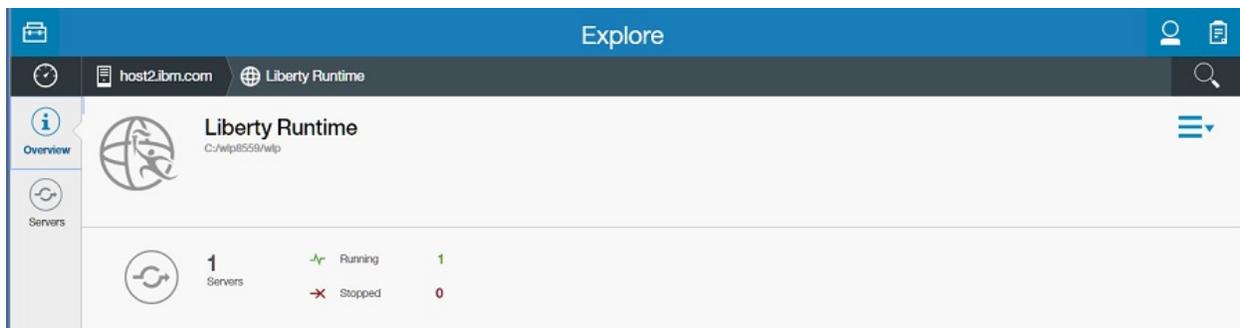
- Select a link on the **Hosts** panel, a host,



**Runtimes** on the vertical navigation bar, and then a runtime.

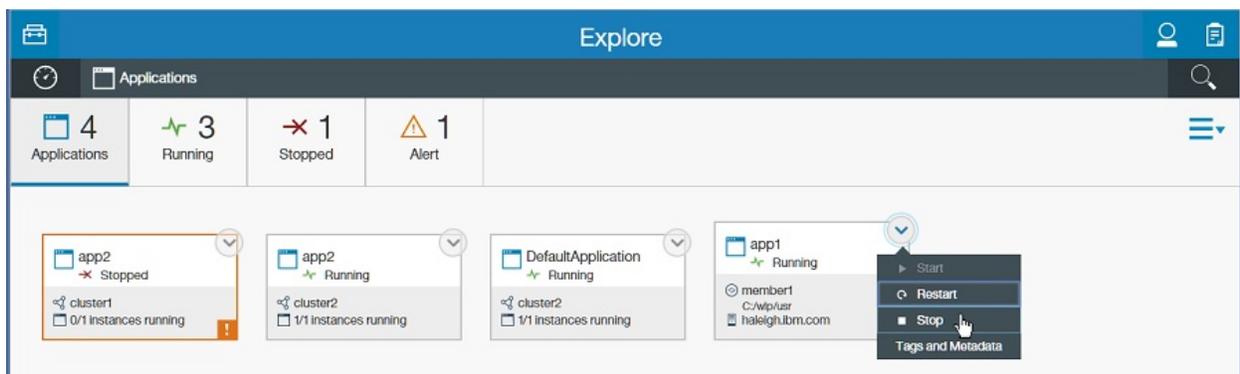
- Select a link on the **Servers** panel, a server, and then **Liberty Runtime** on the horizontal navigation bar.

The Runtime view displays details about the runtime, such as the number and states of servers on the runtime. The runtime details are useful for distinguishing among servers with the same name on the same host.



- Start, stop, or restart a resource.

To start, stop, or restart one resource, select  for the resource, select the available action from the popup dialog, and then confirm the selection.



Alternatively, select  > *one\_or\_more\_resources* > *action\_button*. You can start, stop, or restart multiple resources with this option. For example, to start two stopped servers:

1. When viewing Servers, select .
2. Select two servers in a stopped, partially started, or unknown state.

3. Select the **Start** button.
4. 8.5.5.7 Confirm the selection.

The screenshot shows the VMware vSphere 'Explore' interface. At the top, a summary bar indicates 4 Servers, 2 Running, 2 Stopped, and 1 Alert. Below this, a search filter is applied to 'Type' with 'Alert' selected. The main table displays application instances:

Alert	Name	Location	State	Instances	Tags	Actions
⚠	app2	cluster1	⏹ Stopped	0/1 instances running		⌵
	app2	cluster2	🟢 Running	1/1 instances running		⌵
	DefaultApplication	cluster2	🟢 Running	1/1 instances running	default_app	⌵
	app1	member1 on hale...	⏹ Stopped			⌵

Below the application instances, there are sections for '4 Servers' and '2 Clusters'. The '4 Servers' table shows:

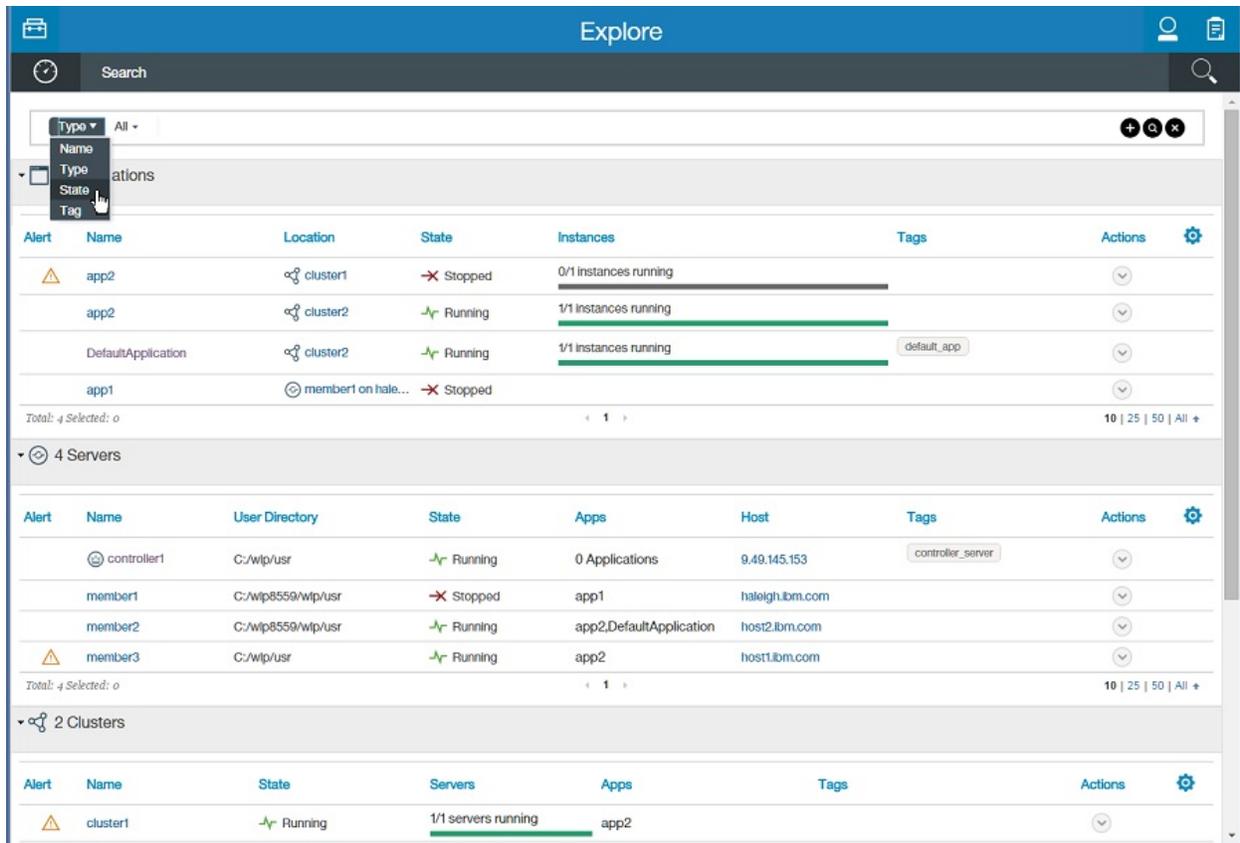
Alert	Name	User Directory	State	Apps	Host	Tags	Actions
	controller1	C:\wlp\usr	🟢 Running	0 Applications	9.49.145.153	controller_server	⌵
	member1	C:\wlp8559\wlp\usr	⏹ Stopped	app1	haleigh.ibm.com		⌵
	member2	C:\wlp8559\wlp\usr	🟢 Running	app2,DefaultApplication	host2.ibm.com		⌵
⚠	member3	C:\wlp\usr	🟢 Running	app2	host1.ibm.com		⌵

The '2 Clusters' table shows:

Alert	Name	State	Servers	Apps	Tags	Actions
⚠	cluster1	🟢 Running	1/1 servers running	app2		⌵

, specify the search criteria, and then select . To add search criteria, select and then specify additional values. To clear the entire search field, select .

The search results list details about resources that fit the search criteria. You can select and then select an available action from the popup dialog to change the resource status or, for hosts, to deploy a server package. To see more details about a resource, select the resource name.



**8.5.5.6** You can filter the search results by entering a string in the search field. For example, enter `er` to show resources that contain the "er" string.

**8.5.5.9** To show or hide columns, select  and the columns to display.

## What to do next

Select  to return to the Explore tool Dashboard. Select a previously viewed resource page on an Explore tool navigation bar to return to that page.

**8.5.5.4** To directly launch the Explore tool in the future, you can use the URL that is shown in the browser when viewing the Explore tool. For example, to directly view information about a particular resource in the future, you can use the URL that is shown in the browser when viewing information about the resource in the Explore tool. Each resource in the Explore tool has a unique URL that you can bookmark and use to directly launch the same resource page.

To return to the Toolbox, select .

## Monitoring metrics in Admin Center

**8.5.5.5**

You can use the Monitor view of the Admin Center Explore tool to track used heap memory, loaded classes, active Java virtual machine (JVM) threads, central processing unit (CPU) usage, and other metrics depending on the resource. The Monitor view shows the metrics graphically in charts. You can customize the Monitor view by selecting the charts to show or hide.

## Procedure

- Open the Monitor view on a server or application.
  1. From the Toolbox, select .
  2. Select a server or application to monitor.
    - To monitor a server, select the **Servers** panel and then a server.
    - To monitor an application, select the **Applications** panel and then an application instance. Or, to monitor an application on a server, select the **Servers** panel, a server, and then an application.
  3. Select  **Monitor** on the vertical navigation bar.

When first displayed, the Monitor view shows the following charts:

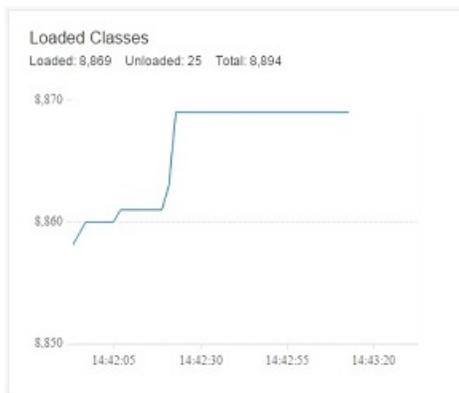
### Used Heap Memory

The Used Heap Memory chart shows the heap memory used by the server in megabytes (MB) every two seconds. The chart also shows the used, committed and maximum megabytes.



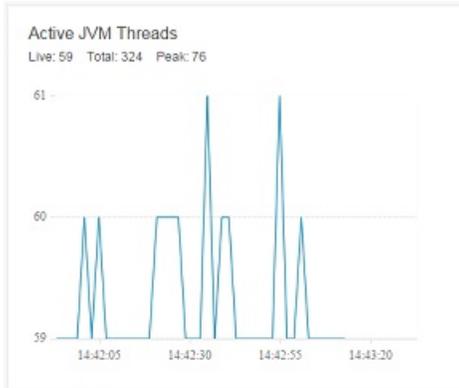
### Loaded Classes

The Loaded Classes chart shows the number of classes loaded every two seconds. The chart also shows the number of loaded and unloaded classes, as well as the total number of classes.



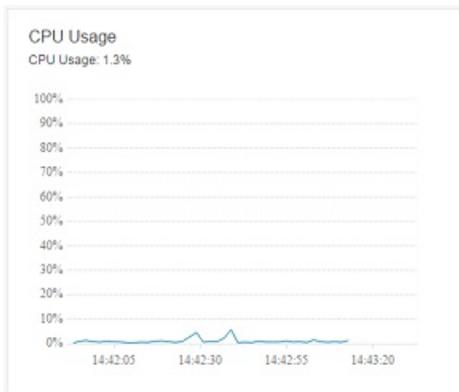
### Active JVM Threads

The Active JVM Threads chart shows the number of JVM threads every two seconds. The chart also shows the number of live, total, and peak threads.



### CPU Usage

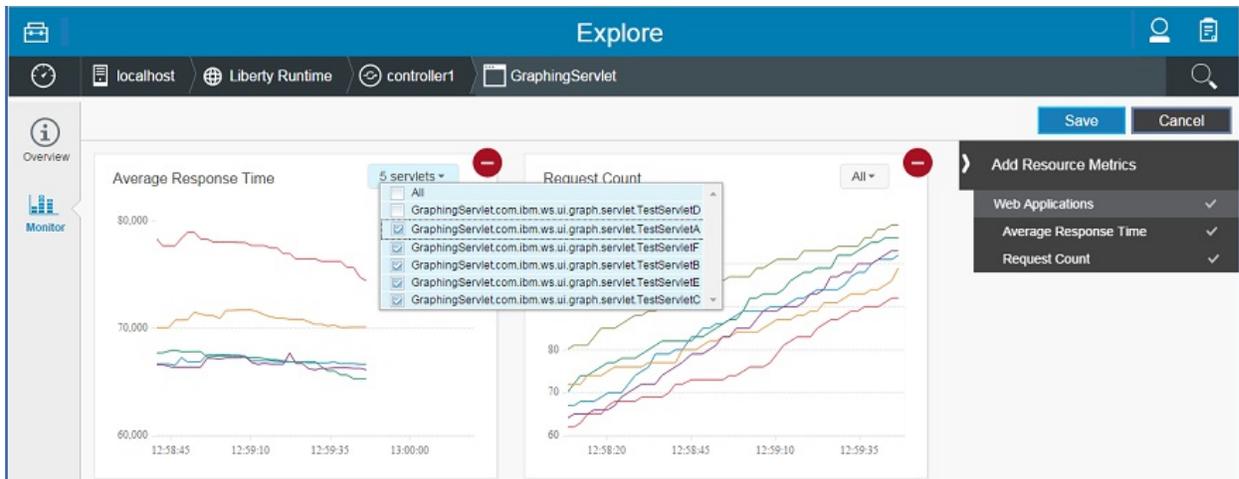
The CPU Usage chart shows the percentage of CPU used every two seconds.



If a server has the `monitor-1.0` feature enabled, the Monitor view also has other charts, depending on the resource:

- Active Sessions
- Active Liberty Threads
- Average Response Time
- Average Wait Time
- Request Count
- Used Connections

**8.5.5.6** The charts available if a server enables the `monitor-1.0` feature have additional configuration options. For example, charts for web applications with multiple servlets, servers with active sessions, or servers with data sources display a drop-down list from which you can select resources to show in the chart.



Select , the resources to show in the chart, and then **Save**.

- Show or hide charts.

Select , the charts to show or hide, and then **Save**. The Monitor view shows or hides the selected charts, depending on whether the chart is shown or hidden when you make the selection.

**8.5.5.6** Your selections are saved for the resource and login user name. When the user opens the Monitor view on the resource in the future, the same chart selections are shown.

- Show or hide chart legends.

If a chart has multiple grid lines, you can choose whether to show or hide the chart legend depending on whether a legend is shown or hidden when you make a selection.

For example, to view a chart legend, select  for the chart and then **Show legend**.

To then hide the legend, select  for the chart and then **Hide legend**.

- **8.5.5.6** View chart data.

In addition to viewing chart data graphically, you can view chart data in a table. Select  for the chart and then **View chart data**.

## Setting and viewing administrative metadata in Admin Center

**8.5.5.5**

You can use the Tags and Metadata dialog of the Explore tool to set and view administrative metadata for server, cluster, host, runtime, and application resources in a Liberty collective. Also, you can view administrative metadata for server, cluster, runtime, and application resources defined in an admin-metadata.xml file in the Explore tool. If a resource has administrative metadata defined in both the Tags and Metadata dialog and an admin-metadata.xml file, the Explore tool displays the resource metadata from both the dialog and the admin-metadata.xml file.

### About this task

The following steps describe how to set or view resource metadata in the Explore tool:

- Set and view administrative metadata in the Tags and Metadata dialog.
- View administrative metadata that is set in an admin-metadata.xml file.

**8.5.5.6** The product stores changes that you save in the Tags and Metadata dialog directly to the collective repository, and not to an admin-metadata.xml file. Changes made to metadata settings in the admin-metadata.xml file are shown in the Tags and Metadata dialog and on the Explore tool resource page when the server to which the admin-metadata.xml file belongs is restarted. Metadata deleted using the Tags and Metadata dialog redisplay in the Explore tool after the server restarts if the deleted

metadata is still defined in the admin-metadata.xml file.

## Procedure

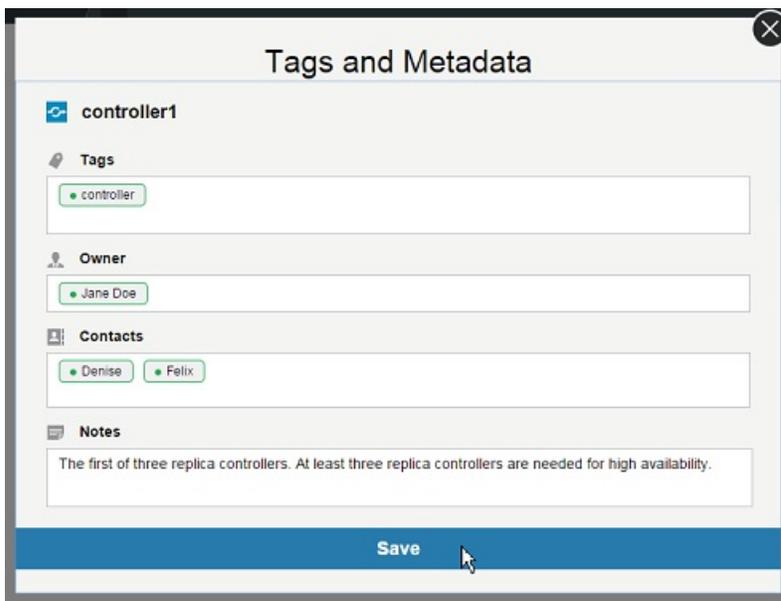
- **8.5.5.6** Set and view administrative metadata for server, cluster, host, runtime, and application resources in the Tags and Metadata dialog of the Explore tool.
  1. From the Toolbox, select .
  2. Select a resource for which to set administrative metadata.
    - For server metadata, select the **Servers** panel and then a server.
    - For cluster metadata, select the **Clusters** panel and then a cluster.
    - **8.5.5.8** For host metadata, select the **Hosts** panel and then a host.
    - **8.5.5.8** For runtime metadata, select the **Servers** panel, a server, and then **Liberty Runtime** or select the **Hosts** panel, a host, **Runtimes**, and then a runtime instance.
    - For application metadata, view application details on a particular server. For example, if app1 is deployed to server1, view the **app1 on server1** details to see the application metadata. If server1 is a member of a cluster, view the **app1 on cluster cluster\_name** details.
      - 8.5.5.8** Each instance of app1 in members of the cluster inherits the app1 application metadata.
  3. Select  or  and then select **Tags and Metadata**.
  4. In the Tags and Metadata dialog, add metadata values to the **Tags**, **Owner**, **Contacts** or **Notes** fields and then select **Save**.

**Tags** A tag is a word that you can use to search for resources. Specify no tags or as many tags as you want. Tags that contain uppercase characters convert to lowercase; thus, MyTag converts to mytag.

**Owner** An owner is typically a person or entity responsible for the metadata. The owner can provide a key for the metadata. Specify no more than one owner.

**Contacts** A contact is a person or entity who can provide information about the resource object. Specify zero or many contacts.

**Notes** A note is arbitrary text. Specify no more than one note.



The metadata is shown in details about the resource after you expand the **Tags and Metadata** link.

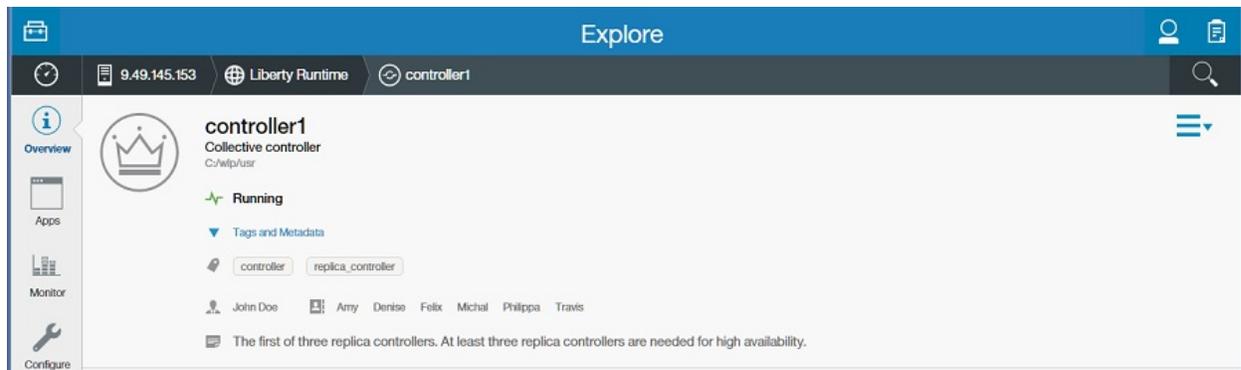
- View administrative metadata for server, cluster, runtime, and application resources defined in an admin-metadata.xml file.

You can see administrative metadata that is set in an `admin-metadata.xml` file in a details or runtime view. “Setting administrative metadata for Liberty resources” on page 1476 describes how to enable an `admin-metadata.xml` file.

For example, suppose a collective controller named `controller1` has the following `admin-metadata.xml` file in its server configuration directory, `$WLP_USER_DIR/servers/controller1`:

```
<admin-metadata>
  <server owner="John Doe">
    <tag>controller</tag>
    <tag>replica_controller</tag>
    <contact>Michal</contact>
    <contact>Felix</contact>
    <contact>Travis</contact>
    <contact>Philippa</contact>
    <contact>Amy</contact>
    <note>The first of three replica controllers. At least three replica controllers are needed for high availability.</note>
  </server>
</admin-metadata>
```

The metadata is shown in details about the `controller1` server after you expand the **Tags and Metadata** link:



Select the expanded **Tags and Metadata** link to hide the metadata.

## Enabling maintenance mode in Admin Center

8.5.5.7

You can use the Explore tool to enable maintenance mode for a server or host. Enable maintenance mode before you perform diagnostic tests, maintenance, or tuning on a server joined to a collective or on a host registered to a collective. Maintenance mode can prevent the disruption of client requests by routing client traffic targeted for a server that is in maintenance mode to another server. Enabling maintenance mode is a persistent change; a server or host remains in maintenance mode until the mode is disabled.

### About this task

The following steps describe how to enable or disable maintenance mode:

- Enable maintenance mode for a server or host.
- Disable maintenance mode for a server or host.

For more information about maintenance mode, see “Entering maintenance mode for Liberty collectives” on page 1516.

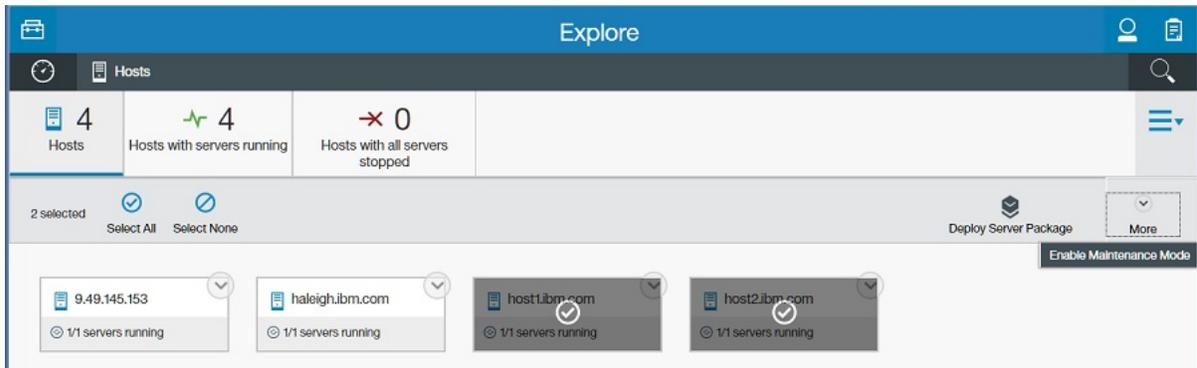
### Procedure

- Enable maintenance mode for a server or host.
  1. Open the Explore tool on Servers or Hosts.
    - a. From the Toolbox, select .
    - b. From the Dashboard, select the **Servers** or **Hosts** panel.

- When viewing Servers or Hosts, select  for a resource and then select **Enable Maintenance Mode** from the popup dialog.

Or, select  > *one\_or\_more\_servers\_or\_hosts* > **Enable Maintenance Mode**. For example, to enable maintenance mode on two hosts:

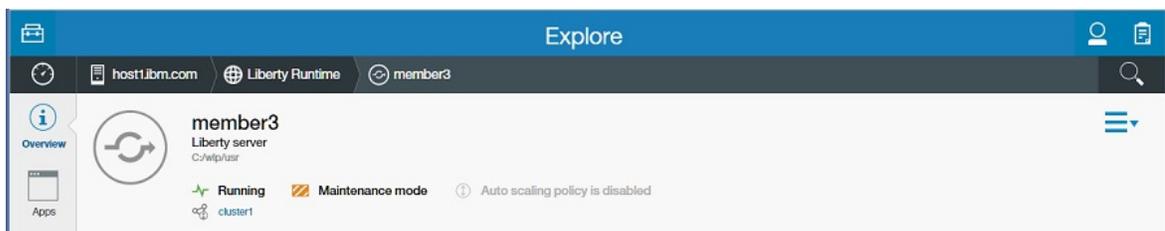
- When viewing Hosts, select .
- Select two registered hosts that are not in maintenance mode.
- Select the **More** button.
- Select the **Enable Maintenance Mode** button.



Enabling maintenance mode on a server might require additional selections:

- If an **Enable maintenance mode** prompt is displayed, select whether to break affinity with active sessions and then select **Enable**. By default, a web server continues to send requests with affinity to a server in maintenance mode. Selecting the **Break affinity with active sessions** toggle causes requests with affinity to a server to be routed to other servers.
- If a server has an enabled scaling policy  and a **Maintenance mode cannot be enabled** prompt is displayed, select **Force** or **Cancel**. When a scaling member is placed into maintenance mode, the scaling controller starts another server to replace the scaling member that is in maintenance mode if another server is needed to meet the scaling policy minimum or to meet current workload demand. If the scaling controller cannot find a server to replace the scaling member, the **Maintenance mode cannot be enabled** prompt is displayed. Selecting **Force** enables maintenance mode for the scaling member without starting alternate servers, which can break auto scaling policies. Selecting **Cancel** does not enable maintenance mode for the scaling member.

When the maintenance mode is enabled on a scaling member, the scaling policy is disabled automatically:



When maintenance mode is enabled on a host, the product attempts to place all servers on the host into maintenance mode, with the host entering maintenance mode regardless of whether its servers do. After a host is in maintenance mode, a scaling controller cannot provision new servers on the host.

- Disable maintenance mode for a server or host.

When viewing Servers or Hosts in the Explore tool, select  for a resource in maintenance mode and then select **Disable Maintenance Mode** from the popup dialog.

Or, select  > *one\_or\_more\_servers\_or\_hosts* > **Disable Maintenance Mode**.

## Deploying resources with Admin Center



8.5.5.2

You can use the Deploy tool to install Liberty server package (archive) files on hosts within a collective. Then, use the Explore tool to manage the servers.

### Before you begin

- The Admin Center feature must be installed and configured on a Liberty server that also includes the collective controller feature and all required security configuration.

To create a Liberty collective that includes the hosts to which you plan to deploy the Liberty installation, see the following topics:

- Configuring a Liberty collective -- To enable Admin Center on the collective controller, the `server.xml` file of the collective controller must include `<feature>adminCenter-1.0</feature>` in the feature manager configuration. Also, the `server.xml` file must set a `host` value in the `httpEndpoint` element; for example, add `host="*"` so all hosts can access the collective controller.
- Registering host computers with a Liberty collective -- The **registerHost** command must include a `hostWritePath` parameter that sets the path to which you want to deploy a server package. You specify this same path for **Target Directory** when using the Deploy tool. If a host is already registered, you can use the **updateHost** command to reset the `hostWritePath` information.

Each host must include Java support for the `jar` utility, and optionally an `unzip` utility, in the environment (path) of the Remote Procedure Call (RPC) user specified during registration of the host.

- The Liberty environment that you want to deploy must be compressed into a server package in the ZIP, JAR, or PAX format. The server package must meet the following requirements:
  - The server package includes, at minimum, a Liberty run time and a server. The server package can include other resources, such as a web application that runs on the server.
  - The top-level directory in the server package must be `wlp`, and it must contain the standard Liberty directories (`bin`, `clients`, `dev`, `lafiles`, `lib`, `templates`, `usr`). The `usr` directory must reside in the default location, and all servers must use the default output directory.
  - Included servers must not contain any collective membership configuration settings or keystore files.

Available tools for packaging archives include:

- The Liberty server **package** command. Sample command syntax is:

```
wlp/bin/server package myServer --include=all | minify --archive=myServer.zip | jar | pax
```
- The **package** action in the WebSphere Developer Tools for Eclipse product.

You might need to customize the installation, for example, by changing port numbers, database connections, or messaging system connections.

### About this task

After you define the Liberty collective and create the server package, use the Deploy tool to install the server package on hosts within the collective.

See “Example: Configuring a collective controller, registering a host, creating a server package, and deploying the server package” on page 1763 for an example of deploying a server package to a localhost Windows computer.

### Procedure

1. Go to the Deploy tool.
  - From the Toolbox, select .

- From details on hosts in the Explore tool, select  > *one\_or\_more\_host\_names* > **Deploy Server Package**.

**8.5.5.4** To directly launch the Deploy tool in the future, you can use the URL that is shown in the browser when viewing the Deploy tool.

2. For **Target Hosts**, select the host computers on which to install the server package. Move target hosts from **Available hosts** to **Selected hosts**.

Each target host must be registered with the collective that is managed by Admin Center. See Registering host computers with a Liberty collective.

3. For **Server Package**, select whether to upload a server package file or use a server package file on a collective controller. Then, specify the file path.
4. For **Target Directory**, specify a target directory for the Liberty installation. If the directory exists, it must be empty. If the directory does not exist, the product creates it as file system permissions permit. For server package ZIP or JAR formats, specify the installation directory. For example, specify `/home/user1/liberty` for the product to upload the server package to `/home/user1` and unzip to the `liberty` directory.

**8.5.5.4** For server package PAX formats, specify the installation directory and PAX file name. For example, specify `/home/user1/liberty/package_name.pax` for the product to expand the archive to the `/home/user1/liberty/package_name.pax` directory.

The RPC user of each target host must have read and write access to the parent of the installation directory.

5. For **KeyStore Password**, specify a password to protect newly generated keystore files containing server authentication credentials. The same password is used for all deployed servers.  
The product generates keystore files in the resources directory of each deployed server.
6. For **Remote Management Credentials**, specify how the collective controller will connect to each target host to remotely manage the deployed servers.

- **8.5.5.4** If all target hosts are registered with the collective controller, you can choose the default option, **Use the connection method and credentials configured for each target host**.

**Restriction:** You cannot use the **Use the connection method and credentials configured for each target host** option to deploy an 8.5.5.3 or earlier server package. The server package must support Liberty 8.5.5.4 or later.

- If all target hosts support SSH, you can choose **Use automatically-generated SSH keys for each server**.
  - If any target host runs on a Windows operating system or otherwise does not support SSH, or if you do not want to use SSH keys, choose **Use the following operating system user name and password on each target host** and specify the operating system login user name and password. The operating system user must possess file system privileges for operating Liberty servers in the installation. All files in a deployed installation are owned by the operating system user who registered the respective target host with the collective. Specifying a different operating system user for **Remote Management Credentials** does not change ownership of the files.
7. For **Password**, specify the password that you used to log in to Admin Center. The operation to join the deployed servers to the collective is run with your Liberty administrative user name and password.
  8. Select **Deploy**.

## Results

The Deploy action runs. Select  on a desktop or tablet, or  on a smartphone, for status on the deployment.

## Example: Configuring a collective controller, registering a host, creating a server package, and deploying the server package

This example describes how to install a Liberty server package on a Windows host within a collective using the Deploy tool.

- Create a collective controller that uses Admin Center and start the collective controller.
- Run the **registerHost** command to register a host computer with the collective controller.
- Create a server package to install using the Deploy tool.
- Install the server package using the Deploy tool.

Configure a collective controller, register a host with the collective controller, and package a server before using the Deploy tool.

- Create a collective controller that uses Admin Center and start the collective controller.

1. Create a server. This example names the server `myController`.

```
wlp/bin/server create myController
```

2. Create a collective controller.

```
wlp/bin/collective create myController --keystorePassword=myControllerPwd
```

3. Open an editor on the `myController` `server.xml` file and make the following changes:

- Add the generated collective controller configuration to the `myController` `server.xml` file. For example, copy output from the collective command and paste it after the `httpEndpoint` element and before `</server>`, the last tag of the `server.xml` file.
- Add the `adminCenter-1.0` feature to the feature manager.

```
<featureManager>  
  <feature>jsp-2.2</feature>  
  <feature>adminCenter-1.0</feature>  
</featureManager>
```

- Add a `host` value to the `httpEndpoint` element of the `myController` `server.xml` file. For example, add `host="*"` so all hosts can access the controller.

```
<!-- To access this server from a remote client add a host  
attribute to the following element, e.g. host="*" -->  
<httpEndpoint id="defaultHttpEndpoint"  
  host="*"  
  httpPort="9080"  
  httpsPort="9443" />
```

- Specify values for `userName` and `userPassword`.

```
<quickStartSecurity userName="admin" userPassword="adminpwd" />
```

**Tip:** If user names or passwords include non-English characters, create the `jvm.options` file for the server and define the default client encoding as UTF-8:

```
-Ddefault.client.encoding=UTF-8
```

If the user registry is in `quickStartSecurity` or `basicRegistry` elements, which store user names and passwords in the `server.xml` file, then save the `server.xml` file in UTF-8 encoding. For information about the `jvm.options` file, see “Customizing the Liberty environment” on page 1565.

4. Start the controller.

```
wlp/bin/server start myController
```

- Run the **registerHost** command to register a host computer with the collective controller.

For this example, the collective controller is running on the localhost computer, which has a hostname of `winHost`. The computer uses a Windows operating system, which does not support SSH, so the command must specify an RPC user and password.

```
wlp/bin/collective registerHost winHost --host=localhost --port=9443 --user=admin --password=adminpwd --rpcUser=myWindowsLoginID
```

The command does the following:

- Registers the localhost computer with the collective controller.
- For user and password, specifies the `userName` and `userPassword` values set in the `myController server.xml` file.
- Specifies the operating system login user for `rpcUser` and the operating system user password for `rpcUserPassword`.
- Sets `hostWritePath` to the path of the directory to which the Deploy tool installs the server package.

When prompted, type `y` to accept the certificate chain.

If you later want to change these settings, you can use the **collective updateHost** command.

- Create a server package to install using the Deploy tool.
  1. If you do not have an existing server to package, run the **create** command to create a new server.
 

```
wlp/bin/server create server1
```
  2. If you have an existing server to package, ensure the server that you want to package is stopped.
  3. Run the **package** command to create the server package.
 

```
wlp/bin/server package server1
```

The command creates a server package named, for example, `C:\wlp\usr\servers\server1\server1.zip`.
- Install the server package using the Deploy tool.
  1. Launch the Deploy tool from the Toolbox or from the Explore tool host page. See “Logging in to Admin Center” on page 1745.
  2. For **Target Hosts**, move the target host, `winHost`, from **Available hosts** to **Selected hosts**.
  3. For **Server Package**, select to use a server package file on a collective controller. Then, specify the file path, `C:\wlp\usr\servers\server1\server1.zip`.
  4. For **Target Directory**, specify the directory set for `hostWritePath` in the **registerHost** command, `c:\wlp_example\member`.
  5. For **KeyStore Password**, specify a password to protect newly generated keystore files containing server authentication credentials. The same password is used for all deployed servers. For example, specify `serverpwd`.
  6. For **Remote Management Credentials**, specify how the collective controller will get the host operating system login credentials to remotely manage the deployed servers. For this example that uses a Windows host computer, you have two choices. You can choose **Use the connection method and credentials configured for each target host** because the target host is registered with the collective controller. Or, you can choose **Use the following operating system user name and password on each target host** and then specify the operating system login user and login user password.
  7. For **Password**, specify the password that you used to log in to Admin Center.
  8. Select **Deploy**.

## What to do next

For details about the status of the deployment on a desktop or tablet, select  on the title bar.

To view the status on a smartphone, select .

On the Background Tasks page, you can view a summary of all running background tasks and access a detailed history of running, stopped, and completed background tasks. See “Monitoring background tasks.”

## Monitoring background tasks



8.5.5.2

You can use the Background Tasks page to check the status of Deploy Installation tasks and view task details.

## About this task

To see details about the progress of steps, errors, or warnings, select a task step in the progress bar or an icon on the Background Tasks page.

## Procedure

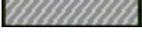
1. Select  on a desktop or tablet, or  on a smartphone.

A drop-down dialog opens, showing active background tasks, which have In Progress or Pending status. The dialog also has a link to **Task Details and History**.

2. To view status on all background tasks, active and completed, select **Task Details and History**.
3. Browse details on tasks in the Background Tasks page.

The Background Tasks page lists running, pending, and completed tasks. Task status is shown by progress bar colors and by icons. No icon is shown if all steps for a task are running or pending.

*Table 124. Background Tasks icon and progress bar.* View the icon and progress bar color to determine the task status.

Icon	Progress bar	Task status
		Successful
		Warning
		Error
		In Progress
		Pending

Each color segment in the progress bar indicates the percentage of each status for the task. The percentage at the end of a progress bar indicates the percentage of hosts that completed the task. Hosts are sub-tasks of a task.

Select a task row to see hosts. If you are deploying a server package to multiple hosts, a list of the hosts is shown under the task.

The icon next to a host name indicates the current status of all operations on the host. Select a host name to see details about operations on the host. If a task, host, or step failed, select the failed step and view error messages.

Background Tasks				
Deploy Installation - liberty.zip	Running	00:00:00:00		0%
 Deploy Installation - liberty.zip	Failed	00:00:00:00		66%
<ul style="list-style-type: none"> <li>^  host2</li> <li>^  host6</li> <li>^  host3</li> <li>^  host1 <ul style="list-style-type: none"> <li>CWWKX0271I: Started to upload file D:/work/liberty/liberty.zip to directory /tmp in... 4/16/2015, 11:33 AM</li> <li>CWWKX0261E: The host authentication information for the host host1 is not avai... 4/16/2015, 11:33 AM</li> </ul> </li> <li>^  host4</li> <li>^  host5</li> </ul>				

## What to do next

After you use task details to troubleshoot any errors or warnings, select  to return to the previous page.

## Configuration updates

**8.5.5.0**

You can make updates to the configuration by using the developer tools or from the command line.

### Updating the server.xml file

The server.xml file can be updated either from the developer tools or from the command line. If there are any problems with the configuration, the specific configuration element updates that have problems do not take effect, but other successful updates are implemented.

This behavior can be changed by updating the onError variable from the default value of WARN to FAIL. If the value is set to FAIL, any problem with the configuration update causes the entire update to fail.

**8.5.5.5** Updates occur if you update any files that are included from the server.xml file or configuration in the configDropins directories.

### Restarting the server with an updated configuration

The WebSphere Application Server Liberty runtime environment caches the currently used configuration so that when you restart the server, the server.xml file is not processed unless there are any changes. If the server.xml file is changed, the cached configuration is updated with the new values. If any problems are found in the new configuration, the cached configuration values remain in use. The console log displays a warning message for each configuration element that is still using an older value. For example:

CWWKG0076W: The previous configuration for `httpEndpoint` with id `defaultHttpEndpoint` is still in use.

The server can be started without using cached configuration by running the server script with the `--clean` option.

---

## Liberty and Chef

Chef software is an open source configuration management tool that you can use to create and manage the installation of an Infrastructure as a Service (IaaS). You can use Chef to provision a Liberty installation.

Chef uses cookbooks, which are reusable sets of components that are written in the Ruby programming language. A cookbook provides all the necessary components that are needed to configure an associated piece of software, for example, Apache HTTP Server. An important distinction between using Chef and writing scripts is the ability of Chef to determine the differences between the current software configuration and a new configuration and make only the changes necessary to move from one to the other. For more information, see the online Chef documentation [About Cookbooks](#).

By using Chef, you can create scalable infrastructure with minimal configuration to maintain. You can easily expand your existing infrastructure, for example, by creating and starting a new application server or web server. Chef automatically connects the new servers into the existing infrastructure as necessary.

The `wlp` cookbook installs and configures the WebSphere Application Server Liberty. It provides recipes, resources, and libraries for creating, managing, and configuring Liberty server instances. For more information, see `wlp` cookbook.

To learn more about Chef, see the online Chef documentation [How Chef works](#).

To learn more about using Chef cookbooks, see [Getting started with the Chef cookbooks for Liberty](#).

---

## Liberty: Including configuration information from external xml files in the server.xml file

8.5.5.6

You can use the **include** element to include configuration information from an external xml file in the `server.xml` file.

If you have configuration information in an external xml file, you can use the **include** element to include the configuration information in the `server.xml` file. For example, if you have an xml file, `simpleSecurity.xml`, with the following content:

```
<server>
  <quickStartSecurity userPassword="thePassword"/>
</server>
```

You can use the following method to include the configuration information in `simpleSecurity.xml` file in your `server.xml` file:

```
<server>
  <featureManager>
    <feature>servlet-3.0</feature>
  </featureManager>
  <quickStartSecurity userName="theUser"/>
  <include location="simpleSecurity.xml"/>
</server>
```

The effective configuration is as follows:

```

<server>
  <featureManager>
    <feature>servlet-3.0</feature>
  </featureManager>
  <quickStartSecurity userName="theUser"/>
  <quickStartSecurity userPassword="thePassword"/>
</server>

```

## Conflict handling

You can configure the *onConflict* attribute in the `server.xml` file to handle the value conflict between `server.xml` file and the external file. This attribute can be configured to one of the three values: *Merge*, *Replace*, and *Ignore*.

**Merge** The values are merged together. *Merge* is the default value of the *onConflict* attribute and *Merge* is equivalent to the behavior that you get if you specify all of the conflicting elements in the `server.xml` file. In the previous example, there are two **quickStartSecurity** elements, and they are effectively merged into a single element. The effective configuration is as follows:

```
<quickStartSecurity userName="theUser" userPassword="thePassword"/>
```

For more information about how configuration elements are merged, see “Liberty:Configuration element merging rules.”

### Replace

The value from the included configuration file replaces the conflicting values in the `server.xml` file. In the previous example, the included **quickStartSecurity** element replaces the one from the `server.xml` file, so the effective configuration is as follows:

```
<quickStartSecurity userPassword="thePassword"/>
```

**Ignore** The value from the included file is ignored. In the previous example, the **quickStartSecurity** element from the included file is ignored, so the effective configuration is as follows:

```
<quickStartSecurity userName="theUser"/>
```

---

## Liberty:Configuration element merging rules

8.5.5.6

If a configuration element is specified multiple times in the server configuration, the elements are merged. The following rules apply to configuration merging:

- Singleton elements are always merged. In the following example, all instances of the element in the server configuration are `featureManager` merged to form a single `featureManager` element:

```

<featureManager>
  <feature>servlet-3.0</feature>
</featureManager>
<featureManager>
  <feature>jdbc-4.0</feature>
</featureManager>

```

The effective configuration becomes:

```

<featureManager>
<feature>servlet-3.0</feature>
<feature>jdbc-4.0</feature>
</featureManager>

```

- Factory elements that are specified at the top level of the server configuration are merged if they have the same ID. In the following example, the `dataSource` element with `id= "ds1"` is merged and the `dataSource` element with `id= "ds2"` stays as it is. For example,

```

<dataSource id="ds1" jdbcDriverRef="myDriver"/>
<dataSource id="ds1" jndiName="jdbc/myDriver"/>
<dataSource id="ds2" jdbcDriverRef="myDriver2"/>

```

The effective configuration becomes:

```
<dataSource id="ds1" jdbcDriverRef="myDriver" jndiName="jdbc/myDriver"/>
<dataSource id="ds2" jdbcDriverDref="myDriver2"/>
```

- If a factory element does not have an ID value, it is considered distinct from other elements of the same type without an ID value. Multiple factory elements without ID values are not merged together. In the following example, the dataSource are not merged, so the effective configuration is the same as the specified configuration:

```
<dataSource jdbcDriverRef="myDriver"/>
<dataSource jndiName="jdbc/myDriver"/>
```

The effective configuration becomes:

```
<dataSource jdbcDriverRef="myDriver"/>
<dataSource jndiName="jdbc/myDriver"/>
```

- If the elements that are to be merged have conflicting attributes, the merged element uses the last value that is encountered by the configuration parser. In the following example, the dataSource element with id= "ds1" is merged and the jdbcDriverRef="myDriver2" is used, while jdbcDriverRef="myDriver" is removed.

```
<dataSource id="ds1" jdbcDriverRef="myDriver"/>
<dataSource id="ds1" jdbcDriverRef="myDriver2"/>
```

The effective configuration becomes:

```
<dataSource id="ds1" jdbcDriverRef="myDriver2"/>
```

- If a factory element is nested underneath another element, it is merged with other elements under the same effective parent only. In the following example, the dataSource element with id= "ds1" is merged and the properties.derby.embedded id="props1" element is merged with the other properties.derby.embedded id="props1" element whose parent is alsodataSource id="ds1".

```
<dataSource id="ds1">
  <properties.derby.embedded id="props1" databaseName="myDB"/>
</dataSource>
<dataSource id="ds2">
  <properties.derby.embedded id="props1" user="myUser"/>
</dataSource>
<dataSource id="ds1">
  <properties.derby.embedded id="props1" createDatabase="create"/>
</dataSource>
```

The effective configuration becomes:

```
<dataSource id="ds1">
  <properties.derby.embedded id="props1" databaseName="myDB" createDatabase="create"/>
</dataSource>
<dataSource id="ds2">
  <properties.derby.embedded id="props1" user="myUser"/>
</dataSource>
```

- If a factory element is nested underneath another element and the factory element does not have a specified ID value, special rules apply depending on the cardinality of the nested element. If multiple nested elements of a particular type are expected, the elements are not merged. However, if only a single nested element is expected, the nested elements are merged together. For example,

```
<topLevel>
  <multipleNested enabled="true"/>
  <multipleNested value="1"/>
  <singleNested enabled="false"/>
  <singleNested value="2"/>
</topLevel>
```

The effective configuration becomes:

```
<topLevel>
  <multipleNested enabled="true"/>
  <multipleNested value="1"/>
  <singleNested enabled="false" value="2"/>
</topLevel>
```

- If two factory elements are nested underneath another element and the ID values that do not match, the merging behavior depends on the cardinality of the nested element. If multiple nested elements are expected, the elements are not merged. If a single nested element is expected, the nested elements are merged together despite the conflicting ID values. For example,

```
<topLevel>
  <multipleNested id="1" enabled="true"/>
  <multipleNested id="2" value="1"/>
  <singleNested id="3" enabled="false"/>
  <singleNested id="4" value="2"/>
</topLevel>
```

The effective configuration becomes:

```
<topLevel>
  <multipleNested id="1" enabled="true"/>
  <multipleNested id="2" value="1"/>
  <singleNested id="4" enabled="false" value="2"/>
</topLevel>
```

---

## Chapter 7. Extending Liberty

### 8.5.5.0

You can expand the capability of Liberty by using product extensions. You can write your own Liberty features and install them onto an existing Liberty server, or you can package them for delivery to your users.

#### About this task

### 8.5.5.0

This section describes how to develop features for a product extension, how to install features to the built-in “usr” product extension, and how to use your features in an application server. Liberty provides various System Programming Interfaces (SPIs) that you can use to extend the runtime environment; you can also use more advanced features such as operating the Liberty server from your Java applications programmatically. **8.5.5.0** The Java API documentation for each Liberty SPI is available in a separate .zip file in one of the javadoc subdirectories of the `{wlp.install.dir}/dev` directory.

For an overview of writing product extensions for Liberty, see “Liberty profile: Product extension” on page 967.

For full details of how to extend Liberty, see the following subtopics:

---

### Developing a Liberty feature for Liberty

### 8.5.5.0

A Liberty feature consists of a feature manifest file, and one or more OSGi bundles. The OSGi bundles contain classes and services that provide a particular capability when the feature is installed onto a Liberty server.

#### About this task

You can develop a Liberty feature in either of the following ways:

- Develop the feature manually; see “Developing a Liberty feature manually.”
- Use the WebSphere Application Server Developer Tools; see “Creating a Liberty feature by using developer tools” on page 1782.

For full details on developing Liberty features, see the following subtopics:

### Developing a Liberty feature manually

### 8.5.5.0

You can create a Liberty feature manually and install it to Liberty.

#### About this task

A feature can consist of a single OSGi bundle and a feature manifest file. This example makes a library available to applications so that the external packages are visible on the default application class path. By

copying the feature manifest into the `${wlp.user.dir}/extension/lib/features` directory, and the OSGi bundle into the `${wlp.user.dir}/extension/lib` directory, the feature can be installed to Liberty. Then you can use the feature in your `server.xml` file.

For details about the format of a feature manifest file, see “Liberty feature manifest files” on page 1773.

This example describes how to construct a Liberty feature manually. Alternatively, you can use the WebSphere Application Server Developer Tools. See “Creating a Liberty feature by using developer tools” on page 1782.

## Procedure

To create a Liberty feature manually, complete the following steps:

1. Create an OSGi bundle containing your Java classes, and a bundle manifest file with appropriate OSGi headers, for example to export the Java packages that you want to expose to applications. `Bundle-SymbolicName` is the only required header; this entry specifies a unique identifier for a bundle, based on the reverse domain name convention. It is good practice to specify a version for the bundle, and in this example some Java packages are exported for application use:

```
Bundle-SymbolicName: com.usr.samplebundle
Bundle-Version: 1.0.1
Export-Package: com.usr.samplebundle.pkg1; version="1.0.0",
               com.usr.samplebundle.pkg2; version="1.0.1"
```

2. Use the `jar` command to package the Java classes and the feature manifest file. For example:  
`jar cfm samplebundle.jar MANIFEST.Mf *.class`
3. Create a feature manifest file named `feature-name.mf` which describes the feature to the runtime environment.
  - a. Provide the required manifest headers:
    - `Subsystem-SymbolicName` to specify the identity and visibility of the feature;
    - `Subsystem-Content` to locate the files that comprise the feature;
    - `IBM-Feature-Version` to identify which version of feature support is required by the runtime environment.
  - b. Best practice: Add the optional manifest headers to indicate the applicable version of the subsystem specification (`Subsystem-ManifestVersion`), the version of your feature (`Subsystem-Version`), and a short name of your feature (`IBM-ShortName`). Specifying these values will help you to evolve your feature in the future.
  - c. In the `IBM-API-Package` header, list the packages that are to be exposed on the default class loader for applications.
  - d. Optional: When you create your Liberty feature, you install it into the user product extension, and the packages in your feature can be accessed by any other feature that is installed to the user product extension. To make one or more SPI packages available to features in other product extensions, list the packages in the `IBM-SPI-Package` header.

```
Subsystem-ManifestVersion: 1.0
Subsystem-SymbolicName: com.example.myfeature.sample-1.0; visibility:=public
Subsystem-Version: 1.0.0.qualifier
Subsystem-Type: osgi.subsystem.feature
Subsystem-Content: samplebundle; version="[1,1.0.100]"
IBM-Feature-Version: 2
IBM-API-Package: com.usr.samplebundle.pkg1; type="api",
               com.usr.samplebundle.pkg2; type="api"
IBM-SPI-Package: com.sample.myservice.spi;
IBM-ShortName: sample-1.0
```

4. Copy the bundle into the `${wlp.user.dir}/extension/lib` directory.
5. Copy the feature manifest into the `${wlp.user.dir}/extension/lib/features` directory.

- If you have defined Subsystem-Name and Subsystem-Description headers in the feature manifest file, and have localized the values, copy the localization files specified in the Subsystem-Localization header into the `/${wlp.user.dir}/extension/lib/features/110n` directory.

## Results

After your feature is installed to Liberty, you can add the feature name to the list of configured feature in your `server.xml` file. For example:

```
<featureManager>
  <feature>usr:sample-1.0</feature>
</featureManager>
```

## Liberty feature manifest files

**8.5.5.0**

A Liberty feature consists of a feature manifest file and a collection of one or more OSGi bundles that provide classes and services corresponding to a particular capability in the Liberty profile runtime environment. You can find the introduction of the format of a feature manifest and the meaning of each header in the manifest file.

The feature manifest file in the Liberty profile uses the Subsystem Service metadata format in the OSGi Enterprise R5 specification. A feature is defined by a feature manifest file (`.mf` file) that is stored in the `lib/features` directory, and must use a custom type of Subsystem: **8.5.5.0** `osgi.subsystem.feature`. For more information on OSGi manifest syntax, see section 1.3.2 of the OSGi core specification.

**Note:** In the feature manifest file, the attributes take the form `name=value`, but directives take the form `name:=value`.

The following headers are defined:

*Table 125. Headers of a feature manifest file.*

This table shows the headers of a feature manifest file in the Liberty profile. The first column shows a list of headers. The second column shows the description of each header, and the third column states whether the header is required.

Header	Description	Required?
Subsystem-ManifestVersion	The version format for the feature manifest file. Must be set to 1.	No
Subsystem-SymbolicName	The symbolic name of the feature and any attributes or directives.	Yes
Subsystem-Version	The version of the feature. See the OSGi core specification section 3.2.5 for the details of how this is defined.	No
Subsystem-Type	The subsystem type for the feature. All features are currently of the same subsystem type: <code>osgi.subsystem.feature</code> .	Yes
Subsystem-Content	The subsystem content of the feature. This is a comma separated list of bundles and subsystems that are required to run this feature. If you want to allow the auto feature to be configured in the <code>server.xml</code> file, you must have the capability header containing the required features, and also define them in the subsystem content.	Yes
Subsystem-Localization	The location of the localization files for the feature.	No

Table 125. Headers of a feature manifest file (continued).

This table shows the headers of a feature manifest file in the Liberty profile. The first column shows a list of headers. The second column shows the description of each header, and the third column states whether the header is required.

Header	Description	Required?
Subsystem-Name	A short, human readable name for the feature. This value can be localized.	No
Subsystem-Description	A description of the feature. This value can be localized.	No
IBM-Feature-Version	The version of this subsystem type. Must be set to 2.	Yes
IBM-Provision-Capability	The capability header that describes whether a feature can be provisioned automatically.	No
IBM-API-Package	The API packages that are exposed to applications by this feature, features in other product extensions, and the Liberty kernel.	No
IBM-API-Service	The OSGi services that are exposed to OSGi applications by this feature.	No
IBM-SPI-Package	The SPI packages that are exposed by this feature to features in other product extensions, and the Liberty kernel.	No
IBM-ShortName	The short name of the feature.	No
IBM-AppliesTo	The Liberty version that this feature applies to.	No
Subsystem-License	The license type for this feature.	No
IBM-License-Agreement	The prefix of the location of the license agreement files.	No
IBM-License-Information	The prefix of the location of the license information files.	No
IBM-App-ForceRestart	Specifies that applications are to be restarted when the feature is installed to, or uninstalled from, a running server.	No

## Subsystem-SymbolicName

The syntax for this header matches the `Bundle-SymbolicName` syntax for a bundle. It has a symbolic name that follows the package names style syntax, and can optionally take a set of attributes and directives.

**8.5.5.0** The following attributes are supported:

- **superseded**. This attribute indicates whether this feature is superseded by one or more features or items of functionality. It takes one of the following values:
  - `true` - The feature is superseded.
  - `false` - The feature is not superseded.

This attribute is optional; the default value is `false`.

For more information, see [Superseded features](#).

- **superseded-by**. This attribute specifies a comma-separated list of the features that supersede this feature, if any, and is optional.

**8.5.5.0** The following directive is supported:

- **visibility**. This directive takes one of the following values:

- `public` - Feature considered to be API. The feature is supported by the developer tools, for use in the `server.xml` file, and output in messages.
- `protected` - Feature considered to be SPI. The feature is not supported by the developer tools, for use in the `server.xml` file, or output in messages. The feature is provided so extenders can use it to build higher-level features.
- `private` - (default) The feature is product internals. The feature is not supported for use in the `server.xml` file or to be referenced by extender features. The feature can be changed at any time, including between fix packs.

For example:

```
Subsystem-SymbolicName: com.ibm.example.feature-1.0;
visibility:=public; superseded=true; superseded-by="com.ibm.example.feature-2.0"
```

**8.5.5.0** If a feature name in the `superseded-by` list is surrounded by brackets, `[]`, this feature is separated from the superseding feature. In the following example, feature `appSecurity-1.0`, which contains features `servlet-3.0` and `ldapRegistry-3.0`, is superseded by feature `appSecurity-2.0`, which does not contain `servlet-3.0` and `ldapRegistry-3.0` features:

```
IBM-ShortName: appSecurity-1.0
Subsystem-SymbolicName: com.ibm.websphere.appserver.appSecurity-1.0; visibility:=public;
superseded=true; superseded-by="appSecurity-2.0, [servlet-3.0], [ldapRegistry-3.0]"
```

For more information, see `Separated features`.

**Best practice:** If the developer tools must show the feature, it must be `public`. If the feature is available only to trusted parties, it must be `protected`. If the feature is internal and subject to change at any time, it must be `private`.

- **8.5.5.6** **singleton**. This directive takes one of the following values:
  - `True`. The feature is a singleton.
  - `False`. The feature is not a singleton.

The **singleton** directive is optional. The default value is `False`.

This directive is used to declare that a particular feature is a singleton. A singleton means that only one version of a given feature can be loaded into the runtime at a time. By default, features are not singletons. If the feature is a singleton and multiple versions of a given feature are required by the server configuration, then the runtime attempts to find a common version that is tolerated by all requiring features. For more information on version toleration, see the **ibm.tolerates** directive under `Subsystem-Content`.

When a feature is a singleton, then the symbolic name value is in the form "`<singleton feature name>-<singleton version>`", where the name and version are separated by a hyphen. The singleton feature name can contain hyphens, but the characters that follow the last hyphen are interpreted as the singleton version. If the characters that follow the last hyphen are not a valid version, then a singleton version of `0.0.0` is used and the complete symbolic name is used as the singleton name. The singleton version is used when processing `ibm.tolerates` directives under `Subsystem-Content`; for example:

```
Subsystem-SymbolicName: com.ibm.example.feature-1.0;
visibility:=public; singleton=true
```

## Subsystem-Content

This header defines the content of the feature, both for run time and install. It follows the same header syntax as the `Subsystem` specification with the following syntax:

```
Subsystem-Content ::= content ( ',' content )*
content ::= unique-name ( ';' parameter )*
unique-name ::= unique-name (see OSGi core spec section 1.3.2)
```

The unique-name uses the form of the `Bundle-SymbolicName` or `Subsystem-SymbolicName` headers. The following attributes are supported:

- **version** - The range of versions to be matched when you find a bundle. Only bundles in this range are selected. A typical example of the version range is `[1,1.0.100)`.
- **type** - The type of content to be provisioned. You can specify any value to indicate the content type; some types result in bundles being installed and started in the OSGi framework of a server that uses the feature, all types cause the content to be included in an installation package that includes the feature. The following values are predefined:
  - `osgi.bundle` - This is the default value and indicates an OSGi bundle that should be provisioned both into the OSGi framework of the server and an installation package.
  - `osgi.subsystem.feature` - This value indicates that the feature should be provisioned both into the OSGi framework of the server and an installation package. These features need to use the name that is specified in `Subsystem-SymbolicName` header.
  - `jar` - This value indicates that a JAR file should be included in an installation package and is selected by using a combination of a version range, a location value, or both.
  - `file` - This value indicates that the file that is identified in the **location** attribute should be included in an installation package.

#### 8.5.5.0

The following directives are supported:

- **location** - The location of the bundle. For a bundle or JAR type, this value can be a comma-separated list of directories that represent a search path. For any type, this value might be a single entry that points directly to the resource and might be specified as a file URL. Paths might be absolute or relative. Relative paths are resolved relative to the location of the product extension that contains the feature. For a user feature, the default product extension location is used which is `${wlp.user.dir}/extension`. The location of non-default product extensions is declared by the `com.ibm.websphere.productInstall` property in its properties file in the `${wlp.install.dir}/etc/extensions` directory.

For example:

```
Subsystem-Content: com.ibm.websphere.appserver.api.basics; version="[1,1.0.100)"; type=jar; location="dev/api/ibm/,lib/",
                  com.ibm.websphere.appserver.spi.application;
                  location="dev/spi/ibm/com.ibm.websphere.appserver.spi.application_1.0.0.jar"; type="jar",
                  com.ibm.websphere.appserver.spi.application_1.0.0-javadoc.zip;
                  location="dev/spi/ibm/javadoc/com.ibm.websphere.appserver.spi.application_1.0.0-javadoc.zip"; type="file"
```

- **start-phase** - The start phase when the bundle should start during system startup. The **start-phase** directive can take one of the following values:
  - `SERVICE` - This value indicates the earliest phase. By default it maps to a start level of 9.
  - `CONTAINER` - This is the default value if no **start-phase** is provided. It indicates the container phase when application containers are started. By default it maps to a start level of 12.
  - `APPLICATION` - This value indicates the latest phase when applications are started.

Bundles can also be defined to start before or just after these phases by adding `_LATE` to be later, or `_EARLY` to be earlier than the key phase. So if you want to run immediately after the container phase, use `CONTAINER_LATE`, and if you want to run before the `APPLICATION` phase then use `APPLICATION_EARLY`.

- **8.5.5.6** **ibm.tolerates** - Specifies alternative singleton version or versions of a singleton feature, `type=osgi.subsystem.feature`, to be provisioned into the system if there are version conflicts.

The unique-name specifies the symbolic name of the preferred version of a singleton feature. If the including feature is known to work with other singleton versions of a given singleton feature, then these singleton versions can be specified by using the **ibm.tolerates** directive. This gives greater compatibility to the defining feature in the case that other features define conflicting required version values of a given singleton feature.

Singleton versions that are listed in the **ibm.tolerates** directive are only used if a version conflict. The ordering of versions that are listed in the **ibm.tolerates** directive is not significant - any version that is listed in the **ibm.tolerates** directive can be selected to satisfy dependency requirements.

The tolerated version or versions of a given singleton feature must be explicitly listed in the **ibm.tolerates** directive. Use commas to separate a list of tolerated versions. Specifying a version range is not supported.

For example:

```
Subsystem-Content: com.ibm.websphere.appserver.example.featureA-1.1; ibm.tolerates="1.2"; type="osgi.subsystem.feature",
com.ibm.websphere.appserver.example.featureB-1.1; ibm.tolerates="1.2, 1.4, 1.6"; type="osgi.subsystem.feature"
```

**Note:**

Tolerated versions are not transitive. This prevents a feature that your feature depends on from being automatically opted in to supporting a later level of a feature, without testing it.

For example: User feature featureC-1.1 includes sipServlet-1.1 in the Subsystem-Content header of its manifest file. sipServlet-1.1 includes servlet-3.0 and tolerates servlet 3.1. If featureC-1.1 was written before servlet-3.1 existed and then servlet-3.1 was added and tolerated by the feature used by it (sipServlet-1.1), featureC-1.1 should have a say on whether it also tolerated servlet-3.1.

If you configure the server.xml file to have the following two features:

```
<feature>usr:featureC-1.1</feature> // includes: sipServlet-1.1
<feature>websocket-1.0</feature> // this feature requires servlet-3.1
```

You will see an error message that resembles the following displayed:

```
CWWKF0033E: The singleton features servlet-3.0 and servlet-3.1 cannot be loaded at the same time.
The configured features usr:featureC-1.1 and websocket-1.0 include one or more features that cause the conflict.
Your configuration is not supported; update server.xml to remove incompatible features."
```

This error is reported because featureC-1.1 is not opted in to tolerating servlet-3.1, and so has to have servlet-3.0, and websocket-1.0 does not support servlet-3.0 and so has to have servlet-3.1.

The solution is for featureC-1.1 to also directly depend on servlet-3.0 and tolerate servlet-3.1.

   The following directives are supported in version 8.5.5.4 and later:

- **ibm.zos.extended.attributes** - Sets the extended attributes to the specified value for the associated file. The value can be any combination of 'a', 'l', 'p', and 's'. Summary of the value options:
  - a = APF authorized
  - p = Program controlled
  - s = Shared address space
  - l = Shared library
- **ibm.file.encoding** - Converts the associated file from ASCII encoding to the encoding type specified. The **ibm.file.encoding** directive can take the value "ebcdic", which converts the ASCII encoded file to EBCDIC encoding.

        The following directive is supported in version 8.5.5.4 and later:

- **ibm.executable** - Adds the execute permission to the associated file, according to the current umask setting, when the value is set to "true". Any other value results in no action taken. The following table shows the current umask and which class gets the execute permission.

Table 126. Examples of umask values and classes with execute permissions set by ibm.executable

Umask	Execute permissions granted to class
022	owner, group, other
023	owner, group

Table 126. Examples of umask values and classes with execute permissions set by `ibm.executable` (continued)

Umask	Execute permissions granted to class
055	owner

## Subsystem-Localization

This header specifies the location of the localization files for the feature.

For example:

```
Subsystem-Localization: OSGI-INF/110n/loc
```

## Subsystem-Name

Use this header to supply a short, human readable name for the feature. You can specify either a literal string or a property name. If you specify a property name, the value can be localized.

For example

```
Subsystem-Name: %name
```

where the value of `name` is defined in a properties file at the location that is specified by the `Subsystem-Localization` header (`loc.properties` in the previous example), in the following format:

```
name=feature_name
```

## Subsystem-Description

Use this header to supply a description for the feature. You can specify either a literal string or a property name. If you specify a property name, the value can be localized.

For example

```
Subsystem-Description: %desc
```

where the value of `desc` is defined in a properties file at the location that is specified by the `Subsystem-Localization` header (`loc.properties` in the previous example), in the following format:

```
desc=feature_description
```

## IBM-Provision-Capability

Automatically provisioned features are features that have the `IBM-Provision-Capability` header in the manifest. This header describes other features that must be provisioned for this feature to be automatically provisioned. When you list the other features, use the `Subsystem-SymbolicName` header of the feature. When any features are configured in the `server.xml` file, the runtime checks to see whether any automatically provisioned features have their capabilities satisfied, and if any have, they are automatically provisioned.

The format of the `IBM-Provision-Capability` header uses standard OSGi LDAP filters.

## IBM-API-Package

This header is used to indicate which API packages are visible to applications. It matches the `Export-Package` header syntax. This means it is a comma-separated list of API packages, but each API package can have some attributes.

**8.5.5.0** The following attribute is supported:

- **type** - The type of API package. The **type** attribute takes one of the following values:
  - `spec` - Indicates an API provided by a standard body, such as `javax.servlet` or `org.osgi.framework`.
  - `ibm-api` - Indicates a value-add API provided by IBM.
  - `api` - Indicates a user-defined API. This is the default value.
  - `third-party` - Indicates an API that is visible, but not controlled by IBM. Typically, these are open source packages.
  - `internal` - Indicates non-API packages that must be exposed to applications for them to function. This might be used if Java code is bytecode enhanced, or *weaved*, to add references to internal code at run time.

For example:

```
IBM-API-Package: javax.servlet; type="spec",
                 com.ibm.websphere.servlet.session; type="ibm-api",
                 com.ibm.wsspi.webcontainer.annotation; type="internal"
```

## IBM-API-Service

This header is used to indicate which services from the feature are visible to OSGi applications. The feature must also register the service in the OSGi service registry.

It has the following syntax

```
IBM-API-Service ::= service ( ',' service )*
                  service ::= service-name ( ';' attribute )*
                  service-name ::= unique-name
```

The `service-name` is the Java class or interface name of the service. The attributes are interpreted as the service properties for the services.

For example:

```
IBM-API-Service: com.ibm.example.service.FeatureServiceOne;
                 myServiceAttribute=myAttributeValue,
                 com.ibm.example.service.FeatureServiceTwo
```

If an OSGi application wants to use the services that are provided by the `IBM-API-Service` header, the application must include a blueprint reference to the service in order for the service to be provisioned into the application.

For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<blueprint xmlns="http://www.osgi.org/xmlns/blueprint/v1.0.0">
  <reference id="FeatureServiceOneRef"
            interface="com.ibm.example.service.FeatureServiceOne" />
</blueprint>
```

In order for a service to be usable by a bundle in an OSGi application, the interface package must be available to that bundle, which means the interface package must be specified by an `Import-Package` header in the manifest file of the consuming bundle. The interface package must also be specified by an `Export-Package` header in a feature bundle and specified in the `IBM-API-Package` header of the feature manifest file. The service that is provided by a feature must be registered in the OSGi service registry by using the OSGi `BundleContext` interface or any other mechanism such as Declarative Services or Blueprint. For more information, see “Developing an OSGi bundle with simple activation” on page 1788 and “Composing advanced features by using OSGi Declarative Services” on page 1793.

## IBM-SPI-Package

When you create your own Liberty feature, you install it into the user product extension. All the packages in your feature can be accessed by any other feature that is installed into the user product extension. However, if you want a package in your feature to be accessed by a feature that is installed into another product extension, you must list the package name in the IBM-SPI-Package header.

Any package that is listed in the IBM-SPI-Package header must be exported by a bundle in the Liberty feature, by being listed in the Export-Package header of the bundle manifest file.

## IBM-ShortName

This header is a short name for a feature that you can use to specify a feature in the `server.xml` file. If there is no IBM-ShortName header in the manifest file, then the Subsystem-SymbolicName is used by default. The IBM-ShortName header is only valid for public features.

## IBM-AppliesTo

This header specifies the Liberty version that this feature applies to. Supply a comma-separated list of items, each in the following form:

```
product_id; productVersion=product_version; productInstallType=product_install_type; productEdition=product_editions
```

If you supply more than one item, the value of *product\_id* must be different for each one.

**8.5.5.7** The value of *productVersion* can be either an exact version, such as *8.5.5.7*, or a minimum version, denoted by the version that ends with a plus sign, +, such as *8.5.5.7+*.

The value of *productEdition* can be either a single edition or a comma-separated list of editions that are enclosed in quotation marks.

For example:

```
IBM-AppliesTo: com.ibm.websphere.appserver; productVersion=8.5.5.6; productInstallType=Archive; productEdition="BASE,DEVELOPERS,EXPRESS,ND"
```

## Subsystem-License

This header defines the license type for this feature. If you supply a value for the Subsystem-License header, and do not supply values for the IBM-License-Agreement and IBM-License-Information headers, then the Subsystem-License header value is displayed to the user for acceptance during installation.

If there is a feature that is already installed with the same Subsystem-License header value, then the license is not displayed, and license approval is not sought, during the installation. If dependencies in the Subsystem-Content header mean that there are two or more features being installed that have the same Subsystem-License header value, the user has only to accept the license once during installation.

For example:

```
Subsystem-License: L-JTHS-93TMHH
```

```
Subsystem-License: http://www.apache.org/licenses/LICENSE-2.0.html
```

## IBM-License-Agreement

This header specifies the prefix of the location of the license agreement files. Supply the file path in the subsystem archive to the *LA\_language* files, up to, but not including, the "\_" character (the language code is appended by the installation tool). If this license has not been accepted, the user must accept the license when you install the feature. The license files are copied to the Liberty installation directory.

For example:

```
IBM-License-Agreement: lafiles/LA
```

## IBM-License-Information

This header specifies the prefix of the location of the license information files. Supply the file path in the subsystem archive to the *LI\_language* files, up to, but not including, the "\_" character (the language code is appended by the installation tool). If this license has not been accepted, the user must accept the license when you install the feature. The license files are copied to the Liberty installation directory.

For example:

```
IBM-License-Information: lafiles/LI
```

## IBM-App-ForceRestart

This header causes applications to be restarted when the feature is installed to, or removed from, a running server. This header can take one of the following values:

- `install` - restart applications when the feature is installed.
- `uninstall` - restart applications when the feature is uninstalled.
- `install,uninstall` - restart applications when the feature is installed or uninstalled.

## Example feature manifest file

The following example shows the definition for the `example-1.0` feature. The public visibility attribute allows this feature to be directly specified in server configuration (`server.xml`) files; it will also be included in the drop down list of features that are displayed in **Server Configuration** view of the developer tools and will be available for inclusion in features that are in other product extensions. If this feature is installed into the `usr` product extension of a runtime install, it can be configured into a server by including the following code in the `server.xml` file:

```
<featureManager>  
  <feature>usr:example-1.0</feature>  
</featureManager>
```

Configuration of this feature in a server results in the specified bundle, `com.ibm.example.bundle1`, being installed and started in the OSGi framework of the server runtime environment. The single API package, `com.ibm.example.publicapi`, will be visible to all applications in that server, except for Java EE applications that are configured to not have visibility to the `api` package type. OSGi applications must explicitly import the package if they wish to use it. The two SPI packages, `com.ibm.example.spi.utils` and `com.acme.spi.spiservices`, will be visible to all feature code in the server, as will the API package.

```
IBM-Feature-Version: 2  
Subsystem-ManifestVersion: 1.0  
Subsystem-SymbolicName: com.ibm.example-1.0; visibility:=public  
Subsystem-Version: 1.0.0.qualifier  
Subsystem-Type: osgi.subsystem.feature  
Subsystem-Content: com.ibm.example.bundle1; version="1.0.0"  
Subsystem-Localization: OSGI-INF/l10n/loc  
Manifest-Version: 1.0  
Subsystem-Name: %name  
Subsystem-Description: %desc  
IBM-API-Package: com.ibm.example.publicapi; type="api"  
IBM-SPI-Package: com.ibm.example.spi.utils, com.ibm.example.spi.spiservices  
IBM-ShortName: example-1.0
```

## Auto-provisioning a feature

8.5.5.0

Auto-provisioning allows a feature to have dependencies on features that must be provisioned before it can be provisioned.

## About this task

An auto-provisioned feature is a feature that has dependencies on other features. Because of the dependencies, the lifecycle of the auto-provisioned feature is as follows:

- The feature is provisioned automatically when all required features are provisioned.
- The feature is de-provisioned automatically when any of the required features are de-provisioned.

## Procedure

To configure a feature to be auto-provisioned, follow these steps:

1. Determine which features must be provisioned before the runtime automatically provisions this feature.
2. Add the `IBM-Provision-Capability` to the manifest header. The format of the `IBM-Provision-Capability` header uses standard OSGi LDAP filters.
3. Deploy the feature to the server.

## Results

The feature automatically provisions when the required features are provisioned.

## Example

In the following example, if features `requiredFeature1-1.0` and `requiredFeature2-1.0` are provisioned, this feature is automatically provisioned. If either of these required features are removed from the `server.xml` file, this feature is automatically de-provisioned.

```
IBM-Provision-Capability: osgi.identity; filter="(
&(type=osgi.subsystem.feature)(osgi.identity=requiredFeature1-1.0)", osgi.identity;
filter="(amp;(type=osgi.subsystem.feature)(osgi.identity=requiredFeature2-1.0))"
```

## Automatic installation of auto-provisioned features

If all the required features are also installed, auto-provisioned features can be installed automatically.

To configure a feature to be auto-installed, the `IBM-Install-Policy` header must be added to the feature manifest. The header is optional. If the `IBM-Install-Policy` header is specified, the following values are valid:

- `manual`: The feature is not auto-installed.
- `when-satisfied`: If all required features are installed, the feature is auto-installed.

If the header is not set, then the feature is not auto-installed, which is equivalent to setting the `IBM-Install-Policy` header to `manual`.

## Creating a Liberty feature by using developer tools

8.5.5.0

You can use the WebSphere Application Server Developer Tools to write your own features and install them into an existing Liberty server, or to package them for delivery to your users.

## About this task

To develop a Liberty feature in the WebSphere Application Server Developer Tools, you create a Liberty feature project and target it to the WebSphere Application Server Liberty version 8.5.5 or later.

You add OSGi bundles that contain classes and services that implement the function provided by your Liberty feature. If your feature provides any API packages to OSGi applications, or SPI packages to features in other product extensions, you can declare those packages in the Liberty feature manifest file.

You can export your liberty feature as a compressed file that can be extracted over an existing WebSphere Application Server Liberty to extend its capabilities.

For more information on creating Liberty features, see “Liberty profile: Product extension” on page 967.

Creating a Liberty feature by using WebSphere Application Server Developer Tools is described in more detail in the following subtopics:

### Procedure

1. “Creating a Liberty feature project.”
2. “Adding OSGi bundles to a Liberty feature project” on page 1784.
3. “Specifying API and SPI packages for a Liberty feature project” on page 1784.
4. “Installing a Liberty feature to Liberty V8.5.5” on page 1785.

### Creating a Liberty feature project

**8.5.5.0**

To develop a Liberty feature by using the WebSphere Application Server developer tools, you must create a Liberty feature project in your workspace.

## About this task

A Liberty feature project contains classes and services that implement the function provided by your Liberty feature

### Procedure

To create a Liberty feature project, complete the following steps:

1. Click **File > New > Other > OSGi > Liberty Feature Project** and then click **Next**. The New Liberty Feature Project wizard opens.
2. In the **Project name** field, enter the name of your Liberty feature project.
3. Select a **Target runtime** from the drop down list. The list will include the WebSphere Application Server Liberty 8.5.5 if it is defined in your workspace as an installed runtime environment.
4. Click **Next**. The OSGi Bundles Selection dialog box opens.
5. Select one or more OSGi bundles to add to the Liberty feature project, or click **New Bundle** to create an OSGi bundle to add to the Liberty feature project. You can add further bundles after you have created the Liberty feature project; see “Adding OSGi bundles to a Liberty feature project” on page 1784.

For information on creating an OSGi bundle, see Creating OSGi bundle projects.

6. Click **Finish** to create the Liberty feature project.

### Results

The Liberty feature project is added to your workspace.

## Adding OSGi bundles to a Liberty feature project

8.5.5.0

A Liberty feature includes OSGi bundles that contain classes and services. The classes and services implement the functions that the Liberty feature provides. You can include OSGi bundles in a Liberty feature that was created with the WebSphere Application Server Developer Tools by adding the bundles to the corresponding Liberty feature project.

### Procedure

To add OSGi bundles to a Liberty feature project, complete the following steps:

1. From the Project Explorer view, open the feature manifest file for the Liberty feature project by double-clicking the **Manifest** node in the project hierarchy, indicated by the manifest icon ().
2. In the Contained Bundles pane, click **Add** to select one or more bundles to add to the Liberty feature project, or click **New** to create a new OSGi bundle to add to the Liberty feature project. For information on creating an OSGi bundle, see [Creating OSGi bundle projects](#).
3. (Optional) Specify the version range for the contained bundle by selecting the bundle, clicking **Properties**, and entering the required values in the **Minimum Version** and **Maximum Version** fields.
4. (Optional) Use the **Location** field in the Properties dialog box to specify the location where you want the bundle to be packaged when exported, relative to the product extension installation folder. If you want the bundle to be packaged in more than one location, enter the locations as a comma-separated list. By default, the bundle is packaged in the `/lib` folder.

### Results

The bundle names are added to the Subsystem-Content header in the manifest file. For more information on the headers in the feature manifest file for a Liberty feature, see “Liberty feature manifest files” on page 1773.

## Specifying API and SPI packages for a Liberty feature project

8.5.5.0

Use the Liberty feature manifest file to declare which packages you want to share as an API or SPI with other applications and features in the Liberty runtime environment.

### About this task

A package cannot be declared as an API or SPI unless it is exported by a bundle in the Liberty feature, by being listed in the Export-Package header of the bundle manifest file.

### Procedure

To specify API and SPI packages for a Liberty feature project, complete the following steps:

1. From the Project Explorer view, open the feature manifest file for the Liberty feature project by double-clicking the **Manifest** node in the project hierarchy, indicated by the manifest icon ().
2. To make one or more API packages available to OSGi applications, click **Add** in the IBM API Packages pane.
3. When you create your own Liberty feature, you install it into the user product extension, and all the packages in your feature can be accessed by any other feature that is installed into the user product extension. To make one or more SPI packages available to features in other product extensions, click **Add** in the IBM SPI Packages pane.

4. (Optional) Specify the package version by selecting the package, clicking **Properties**, and entering the required value in the **Version** field.
5. (Optional) For an API package, select the package type from the **Type** list in the Properties dialog box. The type can be one of the following values:
  - `spec` - Indicates an API provided by a standard body, such as `javax.servlet` or `org.osgi.framework`.
  - `ibm-api` - Indicates a value-add API provided by IBM.
  - `api` - Indicates a user-defined API. This is the default value.
  - `third-party` - Indicates an API that is visible, but not controlled by IBM. Typically, these are open source packages.
  - `internal` - Indicates non-API packages that must be exposed to applications for them to function. This might be used if Java code is bytecode enhanced, or *weaved*, to add references to internal code at run time.

## Results

The package names are added to the `IBM-API-Package` and `IBM-SPI-Package` headers in the feature manifest file. For more information on the headers in the feature manifest file for a Liberty feature, see “Liberty feature manifest files” on page 1773.

## Installing a Liberty feature to Liberty V8.5.5

**8.5.5.0**

When you develop a Liberty feature by using the WebSphere Application Server Developer Tools, you need to create a Liberty feature project that packages the Liberty feature. You can use the workbench to install Liberty features to Liberty runtime environments and enable installed features using the server configuration editor. Changes to features already installed on Liberty can be pushed to all respective runtime environments using the **Update Feature** menu option in the workbench.

### Before you begin

Create a Liberty feature project.

**Restriction:** This topic is supported for WebSphere Application Server Liberty V8.5.5. For versions 8.5 or earlier, see “Manually installing a Liberty feature to Liberty V8.5 or earlier” on page 1786 topic.

### Procedure

To install a Liberty feature, complete the following steps:

1. In the **Enterprise Explorer** view, right-click your Liberty feature project and select **Install Feature**.
2. In the **Feature install** wizard and under **Target Runtimes**, select the Liberty runtime environment that you want to install your feature. Click **Finish**.

**Tip:** If the feature is already installed on Liberty, the Liberty entry is no longer an available option in the list of target runtimes. Instead, you should use the **Update Features** menu option (available when you right-click the Liberty feature project in the Enterprise Explorer view) to update any changes to a feature already installed on Liberty.

3. Add the feature name to the list of configured features in your server configuration (`server.xml` file):
  - a. In the Servers view, expand your Liberty server, right-click the **Server Configuration [server.xml]** and select **Open**.
  - b. In the Server Configuration editor, under the **Configuration Structure**, expand **Server Configuration** and select **Feature Manager**.
  - c. Under the **Feature Manager**, select the **Add** button.

- d. In the **Add Features** wizard, search and select your feature with the prefix `usr:` followed by the name of your Liberty feature project, for example, `usr:MyLibertyFeatureProject`. Click **OK**.

In the **Source** tab of the Server Configuration editor, the `server.xml` file displays the newly added feature entry under the `featureManager` node:

```
<featureManager>
  <feature>usr:MyLibertyFeatureProject</feature>
</featureManager>
```

## Results

After installing the Liberty feature, you can find the following file structure in the `${wlp.user.dir}/extension` directory:

```
/lib
  /features
    manifest files
    .
    .
    .
  OSGi bundle JAR files
  .
  .
  .
```

## What to do next

To update changes to a feature already installed on the Liberty runtime environments, use the **Update Features** menu option (available when you right-click the Liberty feature project in the Enterprise Explorer view). A **Progress Information** window opens and the workbench takes a moment to perform this update action.

## Manually installing a Liberty feature to Liberty V8.5 or earlier

**8.5.0.1**

When you develop a Liberty feature by using the WebSphere Application Server Developer Tools, you create a Liberty feature project that packages the Liberty feature in a compressed file. To install the Liberty feature, you must extract the contents of the compressed file to the Liberty environment.

## Before you begin

Create a Liberty feature project.

**Restriction:** This topic is supported for WebSphere Application Server Liberty V8.5 or earlier. For versions 8.5.5, see “Installing a Liberty feature to Liberty V8.5.5” on page 1785 topic.

## About this task

The compressed file has the following structure:

```
/lib
  OSGi bundle JAR files
  .
  .
  .
/features
  manifest file
```

## Procedure

To install a Liberty feature, complete the following steps:

1. In your workspace, right-click your Liberty feature project and select **Export > Liberty Feature**.
2. In the **To ESA file** field, specify the location and name of the compressed file to which you want to export the Liberty feature project.
3. Click **Finish** to export the Liberty feature project to the specified location.
4. Extract the contents of the compressed file to the `${wlp.user.dir}/extension` directory.
5. Add the feature name to the list of configured features in your `server.xml` file; you must prefix the feature name with `usr:`.

For example:

```
<featureManager>
  <feature>usr:sample-1.0</feature>
</featureManager>
```

## Adding OSGi metatype descriptions to a Liberty feature project

You can add OSGi metatype descriptions to a Liberty feature that was created with the WebSphere Application Server Developer Tools by creating a metatype XML file. You can package that file in an OSGi bundle project.

### Procedure

1. From the Project Explorer view, add a folder in the `BundleContent` folder, and name it `OSGI-INF`.
2. Create a folder that is named `metatype` in the `OSGI-INF` folder.
3. Create the metatype XML file in the `metatype` folder.

The metatype XML file must have a `.xml` suffix. You can use any name for the file.

4. Optional: Provide translated strings for your metatype definitions.

- a. Create a folder to contain the translated properties files.

For example, you can create a subfolder that is named `I10n` in the `OSGI-INF` folder, and use the prefix `metatype` for your translated properties files.

- b. In the metatype XML file, specify the location of the folder that you created.

Use the following example as a guide:

```
<box>
<metatype:MetaData xmlns:metatype="http://www.osgi.org/xmlns/metatype/v1.1.0"
  localization="OSGI-INF/I10n/metatype">
</box>
```

## Results

You created a metatype XML file, which you can use to add OSGi metatype descriptions to a Liberty feature.

## What to do next

You can add information to the metatype XML file. For more information about what to add to the file, see “Liberty feature manifest files” on page 1773.

To describe your configuration by using the OSGi metatype service, package the metatype XML file in the `OSGI-INF/metatype` folder of one of your OSGi bundle projects, not in the Liberty feature project. For best results, put the metatype XML file in the same OSGi bundle as the code that receives and processes the configuration values, such as the associated `ManagedService` implementation. For more information, see “Describing configuration by using the OSGi Metatype service” on page 1798.

## Developing an OSGi bundle with simple activation

8.5.5.0

The most straightforward way to control the lifecycle of your OSGi bundle code is to implement the `org.osgi.framework.BundleActivator` interface in one of the classes within your bundle. When the server starts and stops the bundle, the start and stop methods of the `BundleActivator` interface are called.

### About this task

If you are using the WebSphere Application Server Developer Tools, create an OSGi bundle project, and create an OSGi `BundleActivator` class in that project. Then identify your bundle activator class to the OSGi framework by adding the `Bundle-Activator` header to the bundle `MANIFEST.MF` file. For example:  
`Bundle-Activator: com.example.bundle.Activator.`

### Example

```
package com.example.bundle;

import org.osgi.framework.BundleActivator;
import org.osgi.framework.BundleContext;

public class Activator implements BundleActivator {
    public void start(BundleContext context) throws Exception {
        System.out.println("Sample bundle starting");
        // Insert bundle activation logic here
    }

    public void stop(BundleContext context) throws Exception {
        System.out.println("Sample bundle stopping");
        // Insert bundle deactivation logic here
    }
}
```

## Receiving configuration data by using the `ManagedService` interface

8.5.5.0

Liberty configuration is managed by the OSGi Configuration Admin service and can be accessed according to the OSGi Configuration Admin service specification. Sets of configuration properties are identified by a persisted identity (PID) that is used to associate an element in the `server.xml` file, where the PID is used as the element name, with a component that registers to receive the properties.

### About this task

For an OSGi bundle whose lifecycle is managed by using the `BundleActivator` interface, a straightforward way to receive the configuration properties is to implement the `org.osgi.service.cm.ManagedService` interface, which specifies the PID as one its properties.

### Example

#### Remember:

1. In Eclipse, you must select an SPI target runtime from **Window > Preferences > Plug-In Development > Target Platform**.
2. Add the following statement to your `MANIFEST.MF` file:  
`Import-Package: org.osgi.service.cm;version="1.5.0"`
3. Press `Ctrl + Shift + O` to update your bundle activator.

In this example, the Activator class implements the ManagedService interface in addition to the BundleActivator interface, and receives configuration properties by using the updated method. You can provide default property values to simplify what must be specified in the user configuration.

```
public class Activator implements BundleActivator, ManagedService {

    public void start(BundleContext context) throws Exception {
        System.out.println("Sample bundle starting");
        // register to receive configuration
        ServiceRegistration<ManagedService> configRef = context.registerService(
            ManagedService.class,
            this,
            getDefaults()
        );
    }

    public void stop(BundleContext context) throws Exception {
        System.out.println("Sample bundle stopping");
        configRef.unregister();
    }

    Hashtable getDefaults() {
        Hashtable defaults = new Hashtable();
        defaults.put(org.osgi.framework.Constants.SERVICE_PID, "simpleBundle");
        return defaults;
    }

    public void updated(Dictionary<String, ?> properties) throws ConfigurationException {
        if (properties != null)
        {
            String configColor = (String) properties.get("color");
            String configFlavor = (String) properties.get("flavor");
        }
    }
}
```

User configuration for the bundle can optionally be provided in the `server.xml` file, or an included file, by the following entry:

```
<simpleBundle color="red" flavor="raspberry" />
```

**Note:** The element name in the user configuration, `simpleBundle` matches the value of the `org.osgi.framework.Constants.SERVICE_PID` property used in the `ManagedService` registration.

**8.5.5.0** For more advanced configuration use, see “Describing configuration by using the OSGi Metatype service” on page 1798.

## Working with the OSGi service registry

You can create an object and register it as an OSGi service for use by third-party features that are deployed to Liberty.

### About this task

Services are the OSGi lightweight and flexible component model. When you create services and wire them together with Java code, you can use mechanisms such as `ServiceTrackers` to help find the services that you want, and `Declarative Services (DS)` and `Blueprint` to specify the wiring declaratively. Liberty has standardized on using `DS` for wiring, except for a small number of cases where extra flexibility is required.

## Registering OSGi services: 8.5.5.0

You can create an object and register it as an OSGi service for use by third-party features.

### About this task

By using plain old Java code, you can create an object, and then register it as a service using the `BundleContext` class. Because the code has to run, you typically register the object in a `BundleActivator` interface. When you register the object, you can specify what interfaces it provides, and supply a property map. A `ServiceRegistration` object is returned; if necessary, you can use the `ServiceRegistration` object to change the properties at any time. When the service is completed, you use the `ServiceRegistration` object to unregister the service.

To obtain a service, you query the `BundleContext` for a service that implements a required interface and, optionally, supply an LDAP-syntax filter to match the service properties. Depending on the method you call, you can retrieve the best match or all the matches. You can then use the returned `ServiceReference` that provides the properties to do further matching in your code. You can use the `ServiceReference` to get the actual service object. When you have finished using the service, you use the `BundleContext` to release the service.

### Procedure

1. Declare the service interface by adding the following code in your bundle.

```
package com.ibm.foo.simple;

/**
 * Our multifunctional sample interface
 */
public interface Foo
{
}
```

2. Specify the implementation code of the interface.

```
package com.ibm.foo.simple;

/**
 * The implementation of the Foo interface
 */
public class FooImpl implements Foo
{
    public FooImpl()
    {
    }
    public FooImpl(String vendor)
    {
    }

    /**
     * used by the ServiceFactory implementation.
     */
    public void destroy() {
    }
}
```

3. Use the `BundleContext` to register the service, modify the service properties, and unregister the service directly in your code.

```
import java.util.Dictionary;

import org.osgi.framework.BundleContext;
import org.osgi.framework.ServiceRegistration;
```

```

/**
 * Registers and unregisters a Foo service directly,
 * and shows how to modify the service properties in code.
 */
public class FooController
{

    private final BundleContext bundleContext;
    private ServiceRegistration<Foo> sr;

    public FooController( BundleContext bundleContext )
    {
        this.bundleContext = bundleContext;
    }

    public void register(Dictionary<String, Object> serviceProperties) {
        Foo foo = new FooImpl();
        //typed service registration with one interface
        sr = bundleContext.registerService( Foo.class, foo, serviceProperties );
        //or
        //untyped service registration with one interface
        sr = (ServiceRegistration<Foo>)bundleContext.registerService(
            Foo.class.getName(), foo, serviceProperties );
        //or
        //untyped service registration with more than one interface (or class)
        sr = (ServiceRegistration<Foo>)bundleContext.registerService(new String[] {
            Foo.class.getName(), FooImpl.class.getName()}, foo, serviceProperties );
    }

    public void modifyFoo(Dictionary<String, Object> serviceProperties) {
        //with the service registration you can modify the service properties at any time
        sr.setProperties( serviceProperties );
    }

    public void unregisterFoo() {
        //when you are done unregister the service using the service registration
        sr.unregister();
    }

}

```

#### 4. Obtain and return the service from another class:

```

package com.ibm.foo.simple;

import java.util.Collection;

import org.osgi.framework.BundleContext;
import org.osgi.framework.InvalidSyntaxException;
import org.osgi.framework.ServiceReference;

/**
 * A simple Foo client that directly obtains the Foo service and returns it when done.
 */
public class FooUser
{

    private final BundleContext bundleContext;

    public FooUser( BundleContext bundleContext )
    {
        this.bundleContext = bundleContext;
    }

    /**
     * assume there's only one Foo

```

```

    */
    public void useFooSimple() {
        ServiceReference<Foo> sr = bundleContext.getServiceReference( Foo.class );
        String[] propertyKeys = sr.getPropertyKeys();
        for (String key: propertyKeys) {
            Object prop = sr.getProperty( key );
            //think about whether this is the Foo we want....
        }
        Foo foo = bundleContext.getService( sr );
        try {
            //use foo
        } finally {
            //we're done
            bundleContext.ungetService( sr );
        }
    }

    /**
     * Use a filter to select a particular Foo. Note we get a collection back and have to pick one.
     * @throws InvalidSyntaxException
     */
    public void useFooFilter() throws InvalidSyntaxException {
        Collection<ServiceReference<Foo>> srs = bundleContext.getServiceReferences(
            Foo.class, "(service.vendor=IBM)(id='myFoo')" );
        ServiceReference<Foo> sr = srs.iterator().next();
        String[] propertyKeys = sr.getPropertyKeys();
        for (String key: propertyKeys) {
            Object prop = sr.getProperty( key );
            //think about whether this is the Foo we want....
        }
        Foo foo = bundleContext.getService( sr );
        try {
            //use foo
        } finally {
            //we're done
            bundleContext.ungetService( sr );
        }
    }
}

```

## Using OSGi services: **8.5.5.0**

Services can be registered and unregistered asynchronously at any time. Therefore you should call a service for as short a time as possible. You can use the `ServiceTracker` class to track service availability concurrently.

### About this task

If you want to track services, you can create a `ServiceTracker` object by using your bundle context, the interface you want, and the properties you want to match, and then open the tracker. You can query the tracker for the best match or all matches. Make sure that you do not occupy the service after you use it. You do not have to tell the tracker you are done; the tracker caches the matching services internally, and clears them as they are unregistered. When you have finished using the tracker, use the `serviceTracker.close()` method to close it.

### Example

The following example shows how to use a `ServiceTracker` object to track a service:

```

package com.ibm.foo.tracker;

import com.ibm.foo.simple.Foo;

```

```

import org.osgi.framework.BundleContext;
import org.osgi.util.tracker.ServiceTracker;

/**
 * Simplest use of a ServiceTracker to get a service
 */
public class TrackingFooUser
{
    private ServiceTracker<Foo, Foo> serviceTracker;

    public TrackingFooUser( BundleContext bundleContext )
    {
        serviceTracker = new ServiceTracker<Foo, Foo>( bundleContext, Foo.class, null );
        serviceTracker.open();
    }

    public void doFoo() {
        Foo foo = serviceTracker.getService();
        //use foo
        //no need to return it... just don't use it for long.
    }

    public void shutdown() {
        serviceTracker.close();
    }
}

```

## Composing advanced features by using OSGi Declarative Services

**8.5.6.0**

Simple features can be controlled by using bundle activator classes and direct implementation of interfaces such as `ManagedService` and `ServiceTracker`. As relationships between bundles become more complex, it can be better to use facilities such as OSGi Declarative Services (DS) to decompose a feature into individual services. DS (sometimes known as the Service Component Runtime, or SCR) provides lifecycle and injection management of OSGi services.

### About this task

Organizing your feature logic as a set of declarative services has a number of advantages:

- Activation of the service (which includes loading the Java classes that provide the service) can be deferred until the service is used; allowing the server to start quickly and to keep resource use to a minimum.
- A reference to the service is placed into the service registry, even when the service has not been activated, so that dependencies on the service can be resolved.
- Dependencies on other services can be injected at runtime, and activation of the various services will be ordered based on such dependencies.
- A service can be deactivated and reactivated when its service properties change, if required.

Detailed information about use of OSGi Declarative Services is available from a number of online resources, including the OSGi Community Wiki.

This task provides simple descriptions of how to declare your services to DS, how to obtain references to other services, and how to manage configuration properties for each service.

## Declaring your services to OSGi Declarative Services

8.5.5.0

You can use a separate XML file to declare each service within a bundle.

### About this task

The Declarative Services (DS) support operates on declared components, each of which is defined by an XML file in the bundle. When a bundle containing component declarations is added to the framework, DS reads each component declaration and registers provided services in the service registry. DS then manages the lifecycle of the component: controlling its lifecycle based on a combination of declared attributes and satisfied dependencies.

The XML description of components allows DS to resolve service dependencies without requiring the component to be instantiated, or its implementation classes to be loaded. This facilitates late and lazy resource loading, which helps improve server startup and reduce runtime memory footprint.

The XML files that describe the components are listed in the MANIFEST.MF file of the bundle using the Service-Component header, and by convention are located in the /OSGI-INF directory of the bundle.

There are a number of tools that can be used to generate the required XML; the following examples show the XML itself.

This topic describes a simple OSGi bundle using XML to declare its components to DS.

### Procedure

1. Identify your component through its implementation class name.

```
<component>
  <implementation class="com.example.bundle.HelloComponent"/>
</component>
```

2. Declare the service by referencing the name of the interface that it provides. This is the name that will be published to the service registry by DS when the bundle is started.

```
<component>
  <implementation class="com.example.bundle.HelloComponent"/>
  <service>
    <provide interface="com.example.HelloService"/>
  </service>
</component>
```

3. Name the component. The component name also acts as the service “persisted identity”, or PID, which is used to associate configuration properties with the service. Configuration properties with a matching PID will be injected into the component on activation, and whenever the properties are updated.

```
<component name="HelloService">
  <implementation class="com.example.bundle.HelloComponent"/>
  <service>
    <provide interface="com.example.HelloService"/>
  </service>
</component>
```

**Note:** In Liberty, a user can add the following element to the server.xml configuration file, and the properties will be injected into the HelloComponent class.

```
<HelloService firstKey="firstValue" secondKey="secondValue" />
```

4. Package the XML file into the bundle.

For example, the XML file is at the location OSGI-INF/HelloService.xml, and you add a header to the bundle manifest MANIFEST.MF file so that DS can locate the file:

Service-Component: OSGI-INF/HelloService.xml

If multiple components are packaged in the same bundle, the corresponding XML files must be entered as a comma-separated list. For example:

Service-Component: OSGI-INF/HelloService.xml, OSGI-INF/GoodbyeService

5. The Java implementation of the HelloService component is as follows:

```
package com.example.bundle;

import com.example;
import org.osgi.service.component.ComponentContext;

/**
 * This class must be public and have a public default constructor for it to be
 * usable by DS. This class is not required to be exported from the bundle.
 */
public class HelloComponent implements HelloService {
    /**
     * Optional: DS method to activate this component. If this method exists, it
     * will be invoked when the component is activated. Best practice: this
     * should be a protected method, not public or private
     *
     * @param properties
     *       : Map containing service & config properties
     *       populated/provided by config admin
     */
    protected void activate(ComponentContext cContext,
        Map<String, Object> properties) {
        modified(properties);
    }

    /**
     * Optional: DS method to deactivate this component. If this method exists,
     * it will be invoked when the component is deactivated. Best practice: this
     * should be a protected method, not public or private
     *
     * @param reason
     *       int representation of reason the component is stopping
     */
    protected void deactivate(ComponentContext cContext, int reason) {
    }

    /**
     * Optional: DS method to modify the configuration properties. This may be
     * called by multiple threads: configuration admin updates may be processed
     * asynchronously. This is called by the activate method, and otherwise when
     * the configuration properties are modified while the component is
     * activated.
     *
     * @param properties
     */
    public synchronized void modified(Map<String, Object> properties) {
        // process configuration properties here
    }

    /**
     * Service method defined by com.example>HelloService interface
     */
    public void sayHello() {
        System.out.println("Hello");
    }
}
```

## Enabling a service to receive configuration data

8.5.5.0

To enable a service to receive configuration data, you associate the service with a persisted identity, and code the service to receive the data. You can also provide descriptions and default values for this data, and make the labels and descriptions available in several languages.

### About this task

To enable a service to receive configuration data, there are a number of steps involved. Only associating the service with a configuration Admin persisted identity and coding the service to receive configuration properties are mandatory, and might be considered sufficient for embedded scenarios. The remaining steps improve the configuration experience for users.

The steps involved in enabling a service to receive configuration data are described in the following subtopics:

### Procedure

1. Associate the service with a Configuration Admin PID (persisted identity).
2. Code the service to receive the configuration properties during activation and when the configuration is modified.
3. Provide descriptions and default values for configuration metadata.
4. Provide translated strings for configuration property labels and descriptions.

### Associating a service with a persisted identity: 8.5.5.0

You associate a set of configuration properties with its consuming component as described in the OSGi Configuration Admin specification by using the the persisted identity (PID).

### About this task

The OSGi Configuration Admin specification provides a number of association mechanisms, of which the following are most commonly used in Liberty:

#### Register an implementation of `org.osgi.service.cm.ManagedService` or `org.osgi.service.cm.ManagedServiceFactory` directly with the OSGi Configuration Admin service (CA)

This is most commonly used in low-level kernel bundles, where service management through OSGi Declarative Services (DS) or Blueprint is not available at bundle start time. The registration specifies the PID that identifies the configuration set to be received.

#### Define a service to DS

This is the most common way for services in feature bundles to receive their configuration. The service name is used as the PID to associate configuration data. DS receives the configuration set from CA and passes it on to the defined service.

### Example

A service might be declared by using the following entry in the project \*.bnd file:

```
Service-Component: com.ibm.ws.transaction; \  
  provide:='com.ibm.tx.config.ConfigurationProvider'; \  
  immediate:='true'; \  
  modified:='modified'; \  
  implementation:=com.ibm.ws.transaction.services.JTMConfigurationProvider
```

This generates the following XML code, which can also be coded by the developer instead of using the **bnd** Service-Component entry:

```
<component name="com.ibm.ws.transaction" xmlns="http://www.osgi.org/xmlns/scr/v1.1.0"
    immediate="true" modified="modified">
    <implementation class="com.ibm.ws.transaction.services.JTMConfigurationProvider" />
    <service>
        <provide interface="com.ibm.tx.config.ConfigurationProvider" />
    </service>
    <property name="service.vendor" value="IBM" />
</component>
```

The component name, `com.ibm.ws.transaction` in this example, is used as the PID for the association of configuration data. If this component does not provide any metadata to describe its configuration, you can specify configuration properties for the component by using that PID in the `server.xml` file, or an included file, by defining an entry of the following form:

```
<com.ibm.ws.transaction made.up.property.key="47">
```

### What to do next

Code the service to receive the configuration properties during activation and when the configuration is modified.

### Coding the service to receive configuration properties: **8.5.5.0**

Configuration properties are available through the `org.osgi.service.component.ComponentContext` object that is provided on the activation method.

### Before you begin

You must complete the task described in “Associating a service with a persisted identity” on page 1796.

### About this task

If properties are updated after activation has occurred, the method used for injection depends on the context that the service provides in its OSGi Declarative Services (DS) declaration.

Generally, it is best to declare a method that is to be used specifically for injection of updated properties by using the **modified** attribute on the service declaration. If a modified method is not available, DS deactivates and then reactivates the service with the new properties.

Deactivating and then activating a service can also cause dependent services to be recycled, and should be avoided unless specifically required. Using the **modified** attribute is the preferred way to receive configuration updates.

### Example

In the previous task, “Associating a service with a persisted identity” on page 1796, you defined a service to DS. The following are examples of activate and modified methods from the DS declaration described in that task.

```
private static Dictionary<String, Object> _props = null;

protected void activate(ComponentContext cc) {
    _props = cc.getProperties();
}

protected void modified(Map<?, ?> newProperties) {
```

```

    if (newProperties instanceof Dictionary) {
        _props = (Dictionary<String, Object>) newProperties;
    } else {
        _props = new Hashtable(newProperties);
    }
}

```

When you get values from the configuration properties, use the following mechanisms to allow some flexibility:

- Code the methods to expect at least the default properties that are included in the same bundle, but to make allowances for user overrides, so that migration of user configuration is not necessary.
- Ignore redundant or unrecognized properties.

The service must be able to operate on the default configuration alone. To provide a reasonable level of function, user overrides must not be mandatory.

### What to do next

Provide descriptions and default values for configuration metadata

## Advanced Configuration

8.5.5.0

Advanced configuration includes information about providing descriptions and the default values for configuration and OSGi Metatype Service Extensions.

The configuration properties for each service can be described in metadata that complies with the OSGi Metatype Service specification. The resulting XML file is packaged into the bundle in the OSGI-INF/metatype directory, in accordance with the specification. For more information, see Providing Descriptions and default values for configuration.

The Liberty runtime and developer tools recognize some extensions to the OSGi Metatype specification for more complex configurations and a better presentation in a user interface. For more information, see OSGi Metatype Service Extensions.

### Describing configuration by using the OSGi Metatype service

8.5.5.0

The configuration properties for each service can be described in metadata that complies with the OSGi Metatype Service specification. The metadata can include default values, translatable names and descriptions, and information to allow validation of input values. The resulting XML file is packaged into the bundle that contains your service, in the OSGI-INF/metatype directory, in accordance with the specification.

### About this task

Providing metadata to describe your configuration is optional, but it does provide the following benefits:

- default values can be separated from the implementation code into the metatype XML file where they are easy to locate;
- appropriate data types and other validation data can be specified for each attribute, allowing validation by the configuration parser and developer tools, and simplifying the code you write to process the attributes;
- your configuration will be included in the XML schema that describes the available configuration to the developer tools and other utilities;

- translatable names and descriptions can be provided for each attribute, and will be displayed in the developer tools.

## Procedure

1. Create an xml file in the OSGI-INF/metatype directory of your bundle and add a namespace declaration for the OSGi Metatype namespaces:

```
<metatype:MetaData xmlns:metatype="http://www.osgi.org/xmlns/metatype/v1.1.0">
</metatype:MetaData>
```

2. Add an object class definition (OCD) element to contain the set of attributes, with an identifier and, optionally, a name and description. Also provide a Designate element to map the OCD to the PID used in your code and the server.xml file.

```
<OCD name="b2c" description="bundle two config" id="b2c-id">
</OCD>
```

```
<Designate pid="testBundleTwo">
<Object ocdref="b2c-id" />
</Designate>
```

3. Add attribute definition (AD) elements for each configuration property, within the OCD. Each attribute needs an identifier which is also used in the server.xml file and in the code that receives the injected configuration. It can optionally have a name and description which can be used by the developer tools and other graphical tools. Specifying a data type allows the runtime environment to validate the input for that type and simplifies your processing code. Specifying a useful default value allows the user-supplied configuration to be minimal, and contains all your configuration defaults in a known location:

```
<AD name="boolProperty" description="a boolean property" id="boolProp"
type="Boolean" default="false" />
```

4. Then you have the following metatype.xml file.

```
<?xml version="1.0" encoding="UTF-8"?>
<metatype:MetaData xmlns:metatype="http://www.osgi.org/xmlns/metatype/v1.1.0" >
```

```
<OCD name="b2c" description="bundle two config" id="testBundleTwo-2-id">
<AD name="textProperty" description="a text property"
id="textProp" type="String" default="default string" />
<AD name="boolProperty" description="a boolean property"
id="boolProp" type="Boolean" default="false" />
<AD name="intProperty" description="an integer property"
id="intProp" type="Integer" default="14" />
</OCD>
```

```
<Designate pid="testBundleTwo-2">
<Object ocdref="testBundleTwo-2-id" />
</Designate>
```

```
</metatype:MetaData>
```

5. Code your service to receive the configuration properties. Without the metatype description, all your properties will be provided as String values and will be processed as follows:

```
String textProp = (String) properties.get("textProp");
Boolean boolProp = Boolean.parseBoolean((String) properties.get("boolProp"));
int intProp = Integer.parseInt((String) properties.get("intProp"));
```

```
String textProp = (String) properties.get("textProp");
Boolean boolProp = (Boolean) properties.get("boolProp");
int intProp = (Integer) properties.get("intProp");
```

And the runtime environment will already have validated that the input values are of the correct types.

## What to do next

Provide translated strings for configuration property labels and descriptions.

## Single versus multiple configuration instances

8.5.5.0

You can also configure multiple configuration instances by using the OSGi metatype services.

As described in the “Describing configuration by using the OSGi Metatype service” on page 1798, you can use OSGi metatype service to support a single set of configuration properties for a given service (as identified by a configuration PID). It is also common to support multiple instances of the same configuration type, for example in the way that the Liberty profile supports multiple entries for applications and data sources. This can be done by providing a metatype definition that tells the Liberty configuration parser, and the Configuration Admin service, that it is dealing with a factory configuration. Also, the class that receives the configuration needs to implement the `org.osgi.service.cm.ManagedServiceFactory` interface.

To support multiple instances of top-level configuration elements in the `server.xml` file as follows:

```
<server>
  <teenager name="joy" age="15" />
  <teenager name="angela" age="18" />
</server>
```

You must define the configuration in metadata by adding a **factoryPid** attribute to the Designate element.

**Note:** A **pid** attribute is still needed if you use a `ManagedServiceFactory` interface to receive the configuration; if you use a declarative service (DS) component, this is not required.

```
<?xml version="1.0" encoding="UTF-8"?>
<metatype:MetaData xmlns:metatype="http://www.osgi.org/xmlns/metatype/v1.1.0"
  xmlns:ibm="http://www.ibm.com/xmlns/appservers/osgi/metatype/v1.0.0">

  <OCD id="teenager-ocd" name="teenager" >
    <AD id="name" name="name" type="String" />
    <AD id="age" name="age" type="Integer" />
  </OCD>

  <Designate factoryPid="teenager" pid="teenager">
    <Object ocdref="teenager-ocd" />
  </Designate>

</metatype:MetaData>
```

The `ManagedServiceFactory` implementation is registered as a `ManagedServiceFactory` service type, with the factory pid as follows:

```
bundleContext.registerService(ManagedServiceFactory.class, new MgdSvcFactoryImpl(), new Hashtable());
defaults.put(org.osgi.framework.Constants.SERVICE_PID, "teenager");
```

The `ManagedServiceFactory` implementation receives a set of properties for each instance of the *teenager* configuration, each one uniquely identified by its own (internally generated) PID which is provided to the `updated()` method as follows:

```
public void updated(String pid, Dictionary<String, ?> properties)
  throws ConfigurationException {
  String name = (String) properties.get("name");
  Integer age = (Integer) properties.get("age");
}
```

If a particular configuration instance is deleted, for example because one of the *teenager* elements is deleted from the `server.xml` file, the `ManagedServiceFactory` implementation is notified through the `deleted()` method, and the pid of the deleted instance is provided. This allows the `ManagedServiceFactory` implementation to keep track of the instances that are valid at any given time.

### Providing default instances of factory configurations: **8.5.5.0**

You can create default instances of your factory configuration when using the OSGi metatype services. One of the design principles of Liberty is to keep user configuration as small and simple as possible. By providing default instances of your factory configurations, you don't have to add these configurations into the `server.xml` file.

#### Example

To provide a default configuration instance, you need to include it in an XML file within your OSGi bundle, and reference the file by using the `IBM-Default-Config` header in the bundle manifest file as follows:

```
IBM-Default-Config: OSGI-INF/wlp/defaultInstances.xml
```

The format of the XML file is the same as that of the `server.xml` file, but you must specify a unique identifier for each instance. For example, to provide a default instance of the *teenager* configuration that is used in the example on the “Single versus multiple configuration instances” on page 1800 topic, the `defaultInstances.xml` file must have the following settings:

```
<server>
  <teenager id="predefined-teen1" name="Susie" age="19" />
</server>
```

The default instance is not exposed to users through the configuration schema, and therefore it is not visible in the development tools; however, you can document the instance so that your users can override the individual attributes in their `server.xml` files as follows:

```
<teenager id="predefined-teen1" age="13" />
```

This line of code will override the **age** attribute of the default instance, but the **name** attribute remains valid.

## Extensions to the OSGi metatype service

**8.5.5.0**

The Liberty runtime environment and developer tools recognize some extensions to the OSGi metatype specification for more complex configurations and a better presentation in a user interface.

### Runtime metatype extensions

Add this namespace to your `metatype.xml` file to use the following extensions:

```
xmlns:ibm="http://www.ibm.com/xmlns/appservers/osgi/metatype/v1.0.0"
```

#### **ibm:alias**

The alias extension is used to define a user-friendly name for the configuration while reducing the risk of clashes in the names of configuration elements in the `server.xml` file.

The following example shows the `ibm:alias` extension:

```

<OCD id="com.ibm.ws.jdbc.dataSource.properties"
  name="%properties"
  description="%properties.desc"
  ibm:alias="properties">
  <AD id="username".../>
</OCD>

```

In this example `properties` is the user-friendly name for the configuration. The alias must be different from the id.

When the `ibm:alias` entry is used in the `server.xml` file, it must be prefixed with the product extension name. The product extension name for extensions that are installed in the default user location is `usr`. For product extensions defined to the Liberty installation by using an `extension-name.properties` file in the `wlp/etc/extension` directory, the product extension name is the name that is chosen for `extension-name`.

For the metatype shown in the previous example, if the feature is installed in the default `usr` location then the following are examples of valid `server.xml` entries:

```

<usr_properties username="JANE"/>
<com.ibm.ws.jdbc.dataSource.properties username="JANE"/>

```

### **ibm:type**

Standard attribute types are defined in the metatype specification. Several IBM extended types are available. For more information, see “Extended types” on page 1803.

### **ibm:reference**

The reference attribute specifies the OCD type that a PID references. It is used only with the `ibm:pid` type and supports nesting of elements in the `server.xml` file; see “Nesting configuration elements” on page 1806.

The following example shows the `ibm:reference` extension: `<AD id="fooRef" type="String" ibm:type="pid" ibm:reference="com.ibm.ws.foo".../>`

### **ibm:final**

The final attribute indicates that the value cannot be specified in the config. Instead, the default value from the metatype is always used. Use `name="internal"` to indicate that tools not display this property.

The following example shows the `ibm:final` extension: `<AD id="foo" name="internal" ibm:final="true" type="String" default=${someVariable}"/>`

### **ibm:variable**

The variable attribute is used to specify a variable to be used for the default value if one is not specified. The behavior is to choose, in order:

- The value that is specified in `server.xml`
- The value that is specified as a system property, for example in `bootstrap.properties`
- The default value from the metatype

The following example shows `ibm:variable`: `<AD id="traceString" ibm:variable="trace.string" default=*.all=enabled".../>`

### **ibm:unique**

The unique attribute indicates that a configuration value must be unique across all attribute definitions that use the same unique attribute group. The following unique attribute groups are supported:

-

`jndiName`: use this group on attributes that register a service by using the `osgi.jndi.service.name` property with the JNDI name. For more information, see “Developing with the JNDI default namespace in a Liberty feature” on page 1819

### default value syntax

You can use `${prop-name}` syntax in default expressions to construct strings out of other configuration properties.

The following example shows a default value syntax:

```
<AD id="httpEndpoint.target"
  name="internal" description="internal use only"
  ibm:final="true" required="false" type="String"
  default="(&virtualHost=${id}) (enabled=true)"/>
```

## Extended types

### Duration

The duration type is used to express a time. It is described in multiple units of time. For example, "1h30m" would be an hour and a half. "1d5h10s" would be 1 day, 5 hours, and 10 seconds. The units are globalized, so users enter the values by using abbreviations from their local language.

For English, the following list shows the available units:

- d - Days
- h - Hours
- m - Minutes
- s - Seconds
- ms - Milliseconds

By default, when using the type duration, the value that is specified by the user is evaluated in milliseconds. For example, "10s" would be a long value of 10000 in the dictionary. Furthermore, if a user specifies a value without any unit, this value will be evaluated in milliseconds. For example, a value of "10" would be evaluated as 10 milliseconds. However, you can also specify the duration type such that it evaluates into a different unit. For example, specifying a value of "10" with `ibm:type="duration(s)"` will be evaluated as 10 seconds, and stored as 10 in the dictionary.

The following list shows the possible types:

- duration(h)
- duration(m)
- duration(s)
- duration(ms)
- duration

There is no difference between specifying duration and duration(ms).

#### Note:

Best practice: Always include a unit in the value, and express the value with the unit that is easiest to read. For example, instead of specifying a value of "7200" with `ibm:type="duration(s)"`, specify the value as "2h".

The following examples show the duration type:

- `<AD id="timeout" type="String" ibm:type="duration(s)".../>`
- `<AD id="timeout" type="String" ibm:type="duration".../>`

### Location

The location type allows UI tools to provide a more helpful presentation of attributes that represent various file and directory locations. It does not affect processing by the runtime environment. The dictionary object is always a String.

The following examples show the possible types:

**location**

References a file. The reference can be an absolute, relative file, or it can be a url to a file.

**location(file)**

References a file by using an absolute or relative file path.

**location(dir)**

References a dir by using an absolute or relative file path.

**location(url)**

References a file at the end of a url.

The following example shows the location type:  
`<AD id="location" name="%appmgr.location.name" description="%appmgr.location.desc" type="String" required="true" ibm:type="location"/>`

**Password**

The password type is used for password fields. When used, the dictionary object is an instance of `com.ibm.wsspi.kernel.service.utils.SerializableProtectedString`. The value of the password field is not logged in the trace file. Developer tools displays the encoding options that can be used for a password field. Valid encoding options are xor and aes.

The following example shows the password type:  
`<AD id="password" type="String" ibm:type="password" .../>`

**Hashed password**

The passwordHash type is similar to the password type and is used for hashed password fields. When used, the dictionary object is an instance of `com.ibm.wsspi.kernel.service.utils.SerializableProtectedString`. The value of the hashed password field is not logged in the trace file. Developer tools displays the encoding options that can be used for a hashed password field. Valid encoding options are xor, aes, and hash.

Validate a new password against a hashed password by using the `PasswordUtil.encode(String, String, Map)` method, with the following parameters:

1. New password.
2. Hash algorithm, which is obtained by calling the `PasswordUtil.getCryptoAlgorithm` method. The hash algorithm must match the algorithm of the hashed password.
3. Properties object, where one of the properties uses `PasswordUtil.PROPERTY_HASH_ENCODED` for the key and the hashed password for the value.

If the return value of `PasswordUtil.encode` is the same as the hashed password, then the passwords match.

The following example shows the passwordHash type:  
`<AD id="hashedPassword" type="String" ibm:type="passwordHash" .../>`

**Pid**

The pid type is used to reference another object in the config. It is used with the `ibm:reference` attribute and supports nesting of elements in the `server.xml`; see “Nesting configuration elements” on page 1806.

The following example shows the pid type:  
`<AD id="fooRef" type="String" ibm:type="pid" ibm:reference="com.ibm.ws.foo" .../>`

## OnError

The onError type results in an instance of the onError enumeration in the dictionary. The possible values are WARN, FAIL, and IGNORE.

The following example shows the onError type:<AD id="errorBehavior" type="String" ibm:type="onError".../>

## User interface metatype extensions

Add this namespace to your metatype.xml file to use the following extensions:

```
xmlns:ibmui="http://www.ibm.com/xmlns/appservers/osgi/metatype/ui/v1.0.0"
```

### ibmui:localization

The localization extension is used to specify the metatype localization file. The metatype localization file is used to look up the translations for labels and descriptions of other UI extensions. In most cases, the value of the ibmui:localization extension matches the localization attribute on the <Metadata> element.

The following example shows the ibmui:localization extension:

```
<OCD id="com.ibm.ws.jdbc.dataSource.properties"
  name="%properties"
  description="%properties.desc"
  ibmui:localization="OSGI-INF/110n/metatype">
  <AD id="username".../>
</OCD>
```

### ibmui:extraProperties

The extraProperties extension is used to indicate that an arbitrary set of configuration attributes can be set on this configuration.

The following example shows the ibmui:extraproperties extension:

```
<OCD id="com.ibm.ws.jdbc.dataSource.properties"
  name="%properties"
  description="%properties.desc"
  ibmui:extraProperties="true">
  <AD id="username".../>
</OCD>
```

The label and description that is associated with extension is looked up in the metatype localization file (if one is specified by using the ibmui:localization extension). For the extension label, first extraProperties.<ocd id>.name and then extraProperties.name keys are checked. For the extension description, first extraProperties.<ocd id>.description and then extraProperties.description keys are checked.

### ibmui:group

The group extension is used to specify that the attribute belongs to a group. In the user interface, the attributes that are annotated with the same group are grouped.

The following examples show the ibmui:group extension:

- <AD id="username" ibmui:group="userInfo".../>
- <AD id="password" ibmui:group="userInfo".../>
- <AD id="port" ibmui:group="hostInfo".../>

The group label and description information are looked up in the metatype localization file (if one is specified by using the ibmui:localization extension). For the group label, first <group>.<ocd id>.name and then <group>.name keys are checked. For the group description, first <group>.<ocd id>.description and then <group>.description keys are checked.

## Nesting configuration elements:

You can use metatype extensions to define configuration that can be expressed as nested XML elements in the `server.xml` file.

### Examples

The following example shows how to support this user configuration in the `server.xml` file:

```
<family mother="jane" father="john">
  <child name="susie" age="8" />
  <child name="danny" age="5" />
</family>
```

The metatype XML uses `ibm:type="pid"` and `ibm:reference` as shown in following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<metatype:MetaData
  xmlns:metatype="http://www.osgi.org/xmlns/metatype/v1.1.0"
  xmlns:ibm="http://www.ibm.com/xmlns/appservers/osgi/metatype/v1.0.0">

  <OCD id="family" name="family">
    <AD id="mother" name="mother" type="String" default="Ma" />
    <AD id="father" name="father" type="String" default="Pa" />
    <AD id="child" name="child" ibm:type="pid" ibm:reference="child-pid"
      required="false" type="String" cardinality="6" />
  </OCD>

  <Designate pid="family">
    <Object ocdref="family" />
  </Designate>

  <OCD id="child" name="child" >
    <AD id="name" name="name" type="String" />
    <AD id="age" name="age" type="Integer" />
  </OCD>

  <Designate factoryPid="child-pid">
    <Object ocdref="child" />
  </Designate>

</metatype:MetaData>
```

The following example show how the code that receives the family properties uses the `ConfigurationAdmin` service to obtain the child property sets:

```
public void updated(Dictionary<String, ?> properties)
  throws ConfigurationException {

  Set<String> pids = new HashSet<String>();
  String mother = "null";
  String father = "null";

  try {
    if (properties != null) {
      mother = (String) properties.get("mother");
      father = (String) properties.get("father");
      String[] children = (String[]) properties.get("child");
      if (children == null || children.length == 0) {
        return;
      }

      // Get the configuration admin service
      ConfigurationAdmin configAdmin = null;
    }
  }
}
```

```

ServiceReference configurationAdminReference =
    bundleContext.getServiceReference(ConfigurationAdmin.class.getName());

if (configurationAdminReference != null) {
    configAdmin = (ConfigurationAdmin)
        bundleContext.getService(configurationAdminReference);
}

for (String childPid : children) {
    pids.add(childPid);
    Configuration config = configAdmin.getConfiguration(childPid);
    String name = (String) config.getProperties().get("name");
    Integer age = (Integer) config.getProperties().get("age");
}
}
}

catch (Exception e) {
    e.printStackTrace();
}
}

```

## Localizing the configuration metadata

### 8.5.5.0

The name and description attributes of each metadata entry can be localized, and the translated strings packaged into language-specific properties files.

### Example

The following example shows how the location of the localized files is specified in the header of the metatype file:

```

<metatype:MetaData xmlns:metatype="http://www.osgi.org/xmlns/metatype/v1.1.0"
    localization="OSGI-INF/I10n/metatype">

```

where OSGI-INF/I10n is the location of the translated properties files in the bundle, and metatype is the prefix of the default language properties file. For example, if the default values, usually in English, are in a file called metatype.properties, then each locale is added with its own suffix: metatype\_fr.properties, metatype\_es.properties and so on.

Unlike the metatype XML file, which must always be in the OSGI-INF/metatype directory, the translated files can be in any location that is within the bundle and specified by the **localization** attribute. It is better to not put the properties files in the OSGI-INF/metatype directory alongside the metatype XML file; the Metatype service attempts to parse anything in that location as an XML file, and although that does not cause a failure, it generates unwanted exceptions in the console. The Liberty convention is to put them in the OSGI-INF/I10n directory, but that is not mandatory.

In the metatype XML file, to show that a value is a localized string you use a percent sign at the start of the value. For example, you might use the following definition in the metatype XML file:

```

<AD name="%client.inactivity.timeout" description="%client.inactivity.timeout.desc"
    id="clientInactivityTimeout" required="false" type="Integer" default="60" />

```

and you might use the following definition in the properties file:

```

client.inactivity.timeout=Client inactivity timeout
client.inactivity.timeout.desc=The maximum duration, in seconds, between transactional requests
from a remote client. Any period of client inactivity that exceeds this timeout results in the
transaction being rolled back in this application server.

```

## Providing an application endpoint

You can make a Liberty feature available as web applications by including one or more web application bundles (WABs) in the feature. A WAB is an OSGi bundle with a Web-ContextPath manifest header.

### Procedure

To enable WABs in your feature's bundles, add the `com.ibm.wsspi.appserver.webBundle-1.0` feature to the Subsystem-Content: header in the `.mf` file of your feature:

```
Subsystem-Content:  
my.user.feature.bundle; version="[1,1.0.100)",  
com.ibm.wsspi.appserver.webBundle-1.0; type="osgi.subsystem.feature"
```

## Securing an application endpoint

0.5.5.0

You can secure your feature's application endpoint by performing the following steps:

### Procedure

1. In the `.mf` file of your feature, add the `com.ibm.wsspi.appserver.webBundleSecurity-1.0` feature to the Subsystem-Content: header. This addition causes any protected servlets (as specified in your feature bundle's `WEB-INF/web.xml` file) to be authenticated, and enables role base authorization. You can also assign users, groups, and special subjects to any roles that are defined in the `WEB-INF/web.xml` file.

```
Subsystem-Content:  
my.user.feature.bundle; version="[1,1.0.100)",  
com.ibm.wsspi.appserver.webBundleSecurity-1.0; type="osgi.subsystem.feature"
```

2. To map roles to users, groups, and special subjects, do the following steps:
  - a. Add the `IBM-Authorization-Roles` header to your OSGi bundle's `MANIFEST.MF` file. The header must specify a name which is the id of a role mapping you specify in the `server.xml` file.  
`IBM-Authorization-Roles: my.feature.role.map`
  - b. In the `server.xml` file, add an `authorization-roles` element to map the role names to users and groups. The `id` attribute of the `authorization-roles` element must have the same value as the `IBM-Authorization-Roles` header in the `MANIFEST.MF` file. Add a `<security-role>` subelement for each role that you want to assign user and groups to.

```
<authorization-roles id="my.feature.role.map">  
  <security-role name="employee">  
    <special-subject type="ALL_AUTHENTICATED_USERS"/>  
  </security-role>  
  <security-role name="manager">  
    <user name="bob"/>  
    <user name="mary"/>  
    <group name="managers"/>  
  </security-role>  
</authorization-roles>
```

## Liberty SPI utilities

Liberty provides service programming interfaces (SPI) to complete various tasks.

### Resource location symbols

0.5.5.0

Liberty user configuration is made more portable through the use of variables that represent symbolic locations. Use of these variables helps to prevent the coding of absolute paths that would make the user configuration brittle and less portable. Feature code that receives configuration properties might have to deal with values that contain such variables.

The location service of Liberty can be used to resolve symbolic locations to physical resources. For example, the symbolic location `${wlp.install.dir}/myFile` can be mapped to the local file `myFile` in the installation directory of Liberty. Most methods return a `WsResource` object that wraps the physical resource, but you can also use the `resolveString` method to transform the symbolic location into a `String` that can be used to obtain a `File` object.

The name of the location service is `com.ibm.wsspi.kernel.service.location.WsLocationAdmin` and it is provided by the Liberty kernel, so you do not have to specify a feature in your `server.xml` file to make it available. **8.5.5.0** The Java API documentation for each Liberty SPI is available in a separate `.zip` file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

## Symbols

The `com.ibm.wsspi.kernel.service.location.WsLocationConstants` class defines symbols that refer to directory locations:

- `/`
- `server.config.dir`
- `server.output.dir`
- `server.workarea.dir`
- `shared.app.dir`
- `shared.config.dir`
- `shared.resource.dir`
- `wlp.install.dir`
- `wlp.server.name`
- `wlp.user.dir`
- `usr.extension.dir`

For the meaning of each symbol, see “Liberty:Directory locations and properties” on page 1434.

## Monitoring local files for changes

**8.5.5.0**

Liberty has highly dynamic behavior, responding to changes in configuration, applications and other resources. Much of this dynamic behavior is based on monitoring of the local file system for changes. The service that performs this monitoring is available to all Liberty features through the `FileMonitor` SPI. The file monitor service is provided by the Liberty kernel, so you do not have to specify a feature in your `server.xml` file to make it available.

### About this task

The `FileMonitor` SPI provides different properties to specify what resources are monitored and with what frequency. You have to implement the `FileMonitor` interface and register the implementation class into the service registry.

**8.5.5.0** The Java API documentation for each Liberty SPI is available in a separate `.zip` file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

### Example

```
...
import com.ibm.wsspi.kernel.filemonitor.FileMonitor;
...

public class MyFileMonitor implements FileMonitor {
```

```

...
private final BundleContext bundleContext;
...
public MyFileMonitor(BundleContext bundleContext) {
    this.bundleContext = BundleContext;
    ...
}

public ServiceRegistration<FileMonitor> monitorFiles(Collection<String> paths, long monitorInterval) {
    ...
    final Hashtable<String, Object> fileMonitorProps = new Hashtable<String, Object>();
    fileMonitorProps.put(FileMonitor.MONITOR_FILES, paths);
    fileMonitorProps.put(FileMonitor.MONITOR_INTERVAL, monitorInterval);
    ...
    return bundleContext.registerService(FileMonitor.class, this, fileMonitorProps);
}
...
}

```

## Configuring tracing and logging for features in the Liberty profile

**8.5.5.0**

You can use the tracing and logging mechanism of the Liberty profile for Liberty features. The logging service is part of the Liberty kernel so you do not have to specify a feature in your `server.xml` file to use it.

### About this task

Liberty provides the following SPIs for integrating tracing and logging in your customized feature code:

#### **com.ibm.websphere.ras**

The `com.ibm.websphere.ras` package provides classes to log messages and trace records, as well as some extension points. In general, feature code can use the `java.util.logging` package to log trace and messages, and to control the output through Liberty logging configuration, but the extended capability of the WebSphere package is sometimes useful and the trace guards are slightly more efficient when trace is disabled.

#### **com.ibm.websphere.ras.annotations**

The `com.ibm.websphere.ras.annotations` package provides annotations for use with classes in the other packages. For example, an `@Sensitive` annotation can be used to prevent the contents of the annotated variable from appearing in trace or message output.

#### **com.ibm.ws.ffdc**

The `com.ibm.ws.ffdc` package provides facilities to write first failure data capture (FFDC) records to assist in debugging unexpected exceptions.

#### **com.ibm.wsspi.logging**

The `com.ibm.wsspi.logging` package provides interception points of log and ffdc records.

**8.5.5.0**

The Java API documentation for each Liberty SPI is available in a separate `.zip` file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

### Procedure

The following steps show you how to configure an example Liberty feature, called `myfeature`, to use the tracing and logging mechanism of Liberty:

1. Specify the location of the message file for the feature `myfeature`, and the name of the group that is required by the `com.ibm.websphere.ras.TraceComponent` class.

```

import java.util.ResourceBundle;

public class myFeatureConstants {

```

```

public static final String TR_RESOURCE_BUNDLE =
    "com.mycompany.myFeature.internal.resources.FeatureMessages";

public static final String TR_GROUP = "myFeature";

public static final ResourceBundle messages = ResourceBundle.getBundle(TR_RESOURCE_BUNDLE);
}

```

2. In the implementation class of the feature service code, call the register() method of the com.ibm.websphere.ras.TraceComponent class to register the implementation class with the trace manager that is provided by Liberty. Then, you can configure the trace manger to track the DS methods of the feature.

```

...
import com.ibm.websphere.ras.Tr;
import com.ibm.websphere.ras.TraceComponent;

public class myFeatureServiceImpl {

    private static final TraceComponent tc = Tr.register(myFeatureServiceImpl.class);

    protected void activate(ComponentContext cc, Map<String, Object> newProps) {
        if (tc.isDebugEnabled()) {
            Tr.debug(tc, "myFeatureComponentImpl activated"); }
        ...
    }
}

```

3. Use the TraceOptions annotation to specify the trace group name and the message bundle name.

```

@TraceOptions(traceGroup = myFeatureConstants.TR_GROUP, messageBundle =
    myFeatureConstants.TR_RESOURCE_BUNDLE)
package com.mycompany.myFeature;

import com.ibm.websphere.ras.annotation.TraceOptions;
import com.mycompany.myfeature.internal.myFeatureConstants;
...

```

### Generating first failure data capture (FFDC) records: **8.5.5.0**

FFDC records include the exception stack and optional additional data that is recorded when an unexpected exception is caught by your code. Methods on the com.ibm.ws.ffdc.FFDCFilter class are used to generate these records, and there are a number of methods that might cause a variety of data to be captured.

#### Example

A typical use of the FFDCFilter class is as follows:

```

try{
    // ... do something
} catch (Exception e) {
    FFDCFilter.processException(e, getClass().getName(), unique-probe-id);
    if (TraceComponent.isAnyTracingEnabled() && tc.isDebugEnabled()) {
        Tr.debug(tc, "Exception when doing something; " + e);
    }
    return;
}

```

Where the source id (class name in this example) and the unique probe id (typically the source code line number) combine to provide the exact location in the source code that generates the resulting record. By default, the records are written to the \${server.output.dir}/logs/ffdc directory.

The file space used by the FFDC records in the case of a persistently occurring exception is limited by automatic filtering of duplicate records. For any matching source id, probe id, and exception name, at most 10 exceptions with unique messages are written per day.

Feature code can contribute data to FFDC records by registering a `com.ibm.ws.ffdc.DiagnosticModule` implementation with the FFDC class. Feature code can also intercept FFDC records by registering a `com.ibm.wsspi.logging.IncidentForwarder` implementation with the FFDC class.

## Adding web services global handlers

8.5.5.4

Components that need to register web services handlers to all the web services end points must implement the Handler interface and register that implementation in the service registry.

### Before you begin

The global handler service is provided either by **jaxws-2.2**, **jaxrs-1.1**,  **jaxrs-2.0**, or **jaxrs-2.0 client**, so you must specify the following feature or feature combinations in your `server.xml` file:

- **jaxws-2.2**
- **jaxrs-1.1**
-  **8.5.5.6** **jaxrs-2.0**
-  **8.5.5.6** **jaxrs-2.0 client**
- **jaxws-2.2** and **jaxrs-1.1**
-  **8.5.5.6** **jaxws-2.2** and **jaxrs-2.0**
-  **8.5.5.6** **jaxws-2.2** and **jaxrs-2.0 client**

### About this task

The Handler SPI provides different properties to specify the `ENGINE_TYPE`, the `FLOW_TYPE`, and the client side (`IS_CLIENT_SIDE`) or the server side (`IS_SERVER_SIDE`) where handlers take effect.

You must implement the Handler interface and register the implementation class into the service registry.

The Java API documentation for each Liberty SPI is available in a separate compressed file in one of the Javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

### Deploying the handler bundle:

You can deploy the handler bundle by using the WebSphere Application Server Developer Tools for Eclipse .

#### Procedure

1. Click **File > New > Other** and then expand **OSGi**.
2. Click **OSGi Bundle Project** and click **Next**. The New OSGi Bundle Project window opens.
3. Enter `MyHandler` as the Project name. In the Target runtime list, select **WebSphere Application Server Liberty**. If no runtime exists, click **New Runtime** to create a WebSphere(r) Application Server Liberty runtime.
4. Clear the **Add bundle to application** ratio.
5. Click **Next** twice and go to the OSGi Bundle page.

6. On the **OSGi Bundle** page, check **Generate an activator, a Java class that controls the life cycle of the bundle**. Leave the **Activator name** as `myhandler.Activator` and click **Finish**.
7. Click **Window > Preferences > Plug-in Development > Target Platform** and select **WebSphere Application Server Liberty with SPI**.

**Note:** Ensure that you have added WebSphere Application Server Liberty runtime in 3 on page 1812.

8. Click **Apply** and click **OK**.
9. Expand **MyHandler > BundleContent > META-INF** and open the `MANIFEST.MF` file by using the **Plug-in Manifest Editor**.
10. Create the `MyHandler` and `MyActivator` classes:

```

...
import com.ibm.wsspi.webservices.handler.Handler;
...

public class MyHandler implements Handler {
    ...
    public void handleFault(GlobalHandlerMessageContext arg0) {
        ...
    }
    public void handleMessage(GlobalHandlerMessageContext msgctxt) throws Exception {
        if (msgctxt.getFlowType().equalsIgnoreCase(HandlerConstants.FLOW_TYPE_OUT)) {
            ...
        }
        ...
    }
    ...
}

public class MyActivator implements BundleActivator {
    ...
    public void start(BundleContext context) throws Exception {

        final Hashtable<String, Object> handlerProps = new Hashtable<String, Object>();
        handlerProps.put(HandlerConstants.ENGINE_TYPE, HandlerConstants.ENGINE_TYPE_JAXWS);
        handlerProps.put(HandlerConstants.FLOW_TYPE, HandlerConstants.FLOW_TYPE_IN);
        handlerProps.put(HandlerConstants.IS_CLIENT_SIDE, true);
        handlerProps.put(HandlerConstants.IS_SERVER_SIDE, true);
        handlerProps.put(org.osgi.framework.Constants.SERVICE_RANKING, 3);
        MyHandler myHandler = new MyHandler();
        context.registerService(Handler.class, myHandler, handlerProps);
        ...
    }
    ...
}

```

11. Click **File > New > Other** and then expand **OSGi**.
12. Click **Liberty Feature Project** and then click **Next**. The **Liberty Feature Project** window opens.
13. Specify `MyHandlerFeature` as the **Project name**.
14. In the **Target runtime list**, select **WebSphere Application Server Liberty** and click **Next**. The **OSGi Bundles Selection Page** opens.
15. On **OSGi Bundles Selection Page**, select **MyHandler 1.0.0** as the **Contained Bundles** and click **Finish**.
16. Modify `Manifest:MyHandler` in `MyHandler` project. Click the `MANIFEST.MF` tab and add `com.ibm.wsspi.webservices.handler` to the `Import-package` element.
17. Right-click the `MyHandlerFeature` project, click **Install Feature** to install the feature to Liberty runtime.
18. Edit the `server.xml` file to enable the `MyHandlerFeature`:

```

<featureManager> .....
<feature>jsp-2.2</feature>
<feature>jaxws-2.2</feature> // you can also use one of the following feature or feature combinations: jaxrs-1.1, jaxrs-2.0,
jaxws-2.2 and jaxrs-1.1, jaxws-2.2 and jaxrs-2.0, jaxws-2.2 and jaxrsClient-2.0
<feature>usr:MyHandlerFeature</feature> .....
</featureManager>

```

## Adding custom scaling listeners

8.5.5.9

You can create a custom scaling listener bundle by using WebSphere Application Server Developer Tools for Eclipse. A custom scaling listener is notified of all pending scaling actions. The listener can then permit or deny the scaling action. It can also decide to handle the action, thus provide a full customization of the scaling behavior.

### Before you begin

Ensure your Liberty installation has the `scalingController-1.0` feature. For information about scaling controllers, see “Setting up auto scaling for Liberty collectives” on page 1503 and “Scaling Controller” on page 950.

### About this task

You must implement the listener interface and register the implementation class into the service registry. Your scaling listener can permit or deny and handle scaling actions.

The Java API documentation for each Liberty SPI is available in a separate compressed file in one of the API documentation subdirectories of the `${wlp.install.dir}/dev` directory.

### Procedure

1. Click **File** > **New** > **Other** and then expand **OSGi**.
2. Click **OSGi Bundle Project** and click **Next**. The New OSGi Bundle Project window opens.
3. Enter `ScalingSPISampleBundle` as the Project name. In the Target runtime list, select **WebSphere Application Server Liberty**. If no runtime exists, click **New Runtime** to create a WebSphere Application Server Liberty runtime.
4. Clear the **Add bundle to application** radio button.
5. Click **Next** twice and go to the OSGi Bundle page.
6. On the OSGi Bundle page, check **Generate an activator, a Java class that controls the life cycle of the bundle**. Leave the **Activator name** as `scalingspisamplebundle.Activator` and click **Finish**.
7. Click **File** > **New** > **Other** and then expand **OSGi**.
8. Click **Liberty Feature Project** and then click **Next**. The Liberty Feature Project window opens.
9. Specify `ScalingSPISampleFeature` as the Project name.
10. In the Target runtime list, select **WebSphere Application Server Liberty** and click **Next**. The OSGi Bundles Selection Page opens.
11. On OSGi Bundles Selection Page, select **ScalingSPISampleBundle 1.0.0** as the **Contained Bundles** and click **Finish**.
12. Click **Window** > **Preferences** > **Plug-in Development** > **Target Platform** and select **WebSphere Application Server Liberty with SPI**.
13. Click **Apply** and click **OK**.
14. Expand **ScalingSPISampleBundle** > **BundleContent** > **META-INF** and open the `MANIFEST.MF` file by using the **Plug-in Manifest Editor**.

15. Select the **Dependencies** tab and add the `com.ibm.wsspi.scaling.action.consumer` and `com.ibm.wsspi.scaling.action.controller` packages to the Imported Packages pane. You might need to press **Ctrl+S** to save the changes.
16. In the `ScalingSPISampleBundle` project, add an implementation class called `ScalingSPISamplePlugin`. This new class implements the `com.ibm.wsspi.scaling.action.consumer.ScalingActionPlugin` interface.

```
package scalingspisamplebundle;

import com.ibm.wsspi.scaling.action.consumer.ScalingActionPlugin;
import com.ibm.wsspi.scaling.action.controller.ScalingActionContext;
import com.ibm.wsspi.scaling.action.controller.ScalingActionContext.ActionType;
import com.ibm.wsspi.scaling.action.controller.ScalingActionContext.ActionDecision;;

/**
 * This a sample Liberty scaling SPI plugin that acts as a template for developing a custom
 * SPI plugin. In this plugin, no actual work is done and the return value to the Liberty Scaling
 * controller is always DEFAULT_ACTION.
 */
public class ScalingSPISamplePlugin implements ScalingActionPlugin {

    /** {@inheritDoc} */
    @Override
    public ActionDecision actionRequired(ScalingActionContext action) {

        ActionDecision returnType = ActionDecision.DEFAULT_ACTION;

        if (action.getActionType() == ActionType.START_SERVER) {
            returnType = startServer(action);
        }
        else if (action.getActionType() == ActionType.CREATE_SERVER) {
            returnType = createServer(action);
        }
        else if (action.getActionType() == ActionType.STOP_SERVER) {
            returnType = stopServer(action);
        }

        return returnType;
    }

    private ActionDecision startServer(ScalingActionContext action) {
        // perform some action to start a server

        return ActionDecision.DEFAULT_ACTION;
    }

    private ActionDecision createServer(ScalingActionContext action) {
        // perform some action to create a server

        return ActionDecision.DEFAULT_ACTION;
    }

    private ActionDecision stopServer(ScalingActionContext action) {
        // perform some action to stop a server

        return ActionDecision.DEFAULT_ACTION;
    }
}
```

17. In the `ScalingSPISampleBundle` project, open the `Activator` class and edit the `start(BundleContext)` method to add code that registers the new listener service.

```
public void start(BundleContext context) throws Exception {
    final Hashtable<String, Object> properties = new Hashtable<String, Object>();
    ScalingSPISamplePlugin scalingSPISamplePlugin = new ScalingSPISamplePlugin();
    context.registerService(ScalingActionPlugin.class, scalingSPISamplePlugin, properties);
}
```

If prompted to import a `HashMap`, select to import `java.util.HashMap`.

18. Right-click the **ScalingSPISampleFeature** project, and click **Install Feature** to install the feature to Liberty runtime.

The **Install Feature** menu option is in the Enterprise Explorer view of the Java EE perspective.

19. Edit the `server.xml` file to enable the `ScalingSPISampleFeature`.

```
...
<featureManager>
  ...
  <feature>scalingController-1.0</feature>
  <feature>usr:ScalingSPISampleFeature</feature>
</featureManager>
...
```

## Exposing REST endpoints within Liberty

8.5.5.4

You can use the REST Handler framework in the Liberty SPI to expose new REST endpoints.

### About this task

The REST Handler framework is for Liberty extenders to use when exposing new REST endpoints. You can expose REST endpoints in an OSGi component, or a set of components.

### Procedure

1. Create an OSGi component that registers itself as listening to a sub-root that appends to `/ibm/api` and implements the `com.ibm.wsspi.rest.handler.RESTHandler` interface; for example:

```
@Component(service = { RESTHandler.class },
            configurationPolicy = ConfigurationPolicy.IGNORE,
            immediate = true,
            property = { "service.vendor=IBM",
                        RESTHandler.PROPERTY_REST_HANDLER_ROOT + "/myTest/abc" })
public class RESTHANDLERTest1 implements RESTHandler {
  ...
}
```

2. Package the component into an OSGi bundle that is part of your extended user feature.

3. Ensure that your feature includes the OSGi subsystem content:

```
com.ibm.websphere.appserver.restHandler-1.0; type="osgi.subsystem.feature"
```

4. Configure SSL certificates in the `server.xml` file.

5. Configure a user or group to the administrator role in the `server.xml` file.

- Map to the administrator role for Liberty
- **z/OS** Map to the administrator role for Liberty on z/OS

6. Start your feature.

Starting the feature starts the REST Handler framework and registers your OSGi component. After the feature starts, you can make calls to `https://<host>:<https_port>/ibm/api/myTest/abc`.

## Including protected features

Your feature can include one or more other features by listing them in the `Subsystem-Content` header of the feature manifest file. Any feature in the same product extension as your own feature can be included; if the included feature is in a different product extension, or in Liberty, it must have public or protected visibility.

The included feature must be specified by its `Subsystem-SymbolicName`, and have a type of `"osgi.subsystem.feature"`; for example:

Subsystem-Content:

```
com.ibm.wsspi.appserver.webBundle-1.0; type="osgi.subsystem.feature",
com.ibm.websphere.appserver.json-1.0; type="osgi.subsystem.feature"
```

For information on Liberty public features, see “Liberty features” on page 826. The following section describes Liberty protected features.

## Liberty protected features

### Application Manager

This feature provides advanced capability for implementing new application containers.

Subsystem-SymbolicName: com.ibm.websphere.appserver.appmanager-1.0.

Provided API and SPI:

- dev/api/ibm/com.ibm.websphere.appserver.api.basics\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.application\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.artifact\_1.0.9.jar

### Classloader service

This feature provides advanced capability for implementing new application containers.

Subsystem-SymbolicName: com.ibm.websphere.appserver.classloading-1.0.

Provided API and SPI:

- dev/spi/ibm/com.ibm.websphere.appserver.spi.classloading\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.artifact\_1.0.9.jar

### Container services

This feature provides advanced capability for implementing new application containers.

Subsystem-SymbolicName: com.ibm.websphere.appserver.containerServices-1.0,

Provided API and SPI:

- dev/spi/ibm/com.ibm.websphere.appserver.spi.containerServices\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.anno\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.artifact\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.javaeedd\_1.0.9.jar

### Transaction manager 1.1

This feature provides a JTA 1.1 compliant transaction manager.

Subsystem-SymbolicName: com.ibm.websphere.appserver.transaction-1.1.

Provided API and SPI:

- dev/api/spec/com.ibm.ws.javaee.transaction.1.1\_1.0.9.jar
- dev/api/ibm/com.ibm.websphere.appserver.api.transaction\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.containerServices\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.anno\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.artifact\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.javaeedd\_1.0.9.jar

### Transaction manager 1.2

This feature provides a JTA 1.2 compliant transaction manager.

Subsystem-SymbolicName: com.ibm.websphere.appserver.transaction-1.2.

Provided API and SPI:

- dev/api/spec/com.ibm.ws.javaee.transaction.1.2\_1.0.9.jar
- dev/api/ibm/com.ibm.websphere.appserver.api.transaction\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.containerServices\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.anno\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.artifact\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.javaeedd\_1.0.9.jar

## Web Bundle

This feature supports the use of web application bundles (WABs) in features. Include this feature if your feature provides an application endpoint, as described in “Providing an application endpoint” on page 1808.

Subsystem-SymbolicName: com.ibm.wsspi.appserver.webBundle-1.0.

Provided API and SPI:

- dev/api/spec/com.ibm.ws.javaee.servlet.3.0\_1.0.9.jar
- dev/api/ibm/com.ibm.websphere.appserver.api.servlet\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.servlet\_1.0.9.jar

## Web Bundle Security

This feature supports the application of security to web bundles; see “Securing an application endpoint” on page 1808.

Subsystem-SymbolicName: com.ibm.wsspi.appserver.webBundleSecurity-1.0.

Provided API and SPI:

- dev/api/spec/com.ibm.ws.javaee.servlet.3.0\_1.0.9.jar
- dev/api/ibm/com.ibm.websphere.appserver.api.servlet\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.servlet\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.containerServices\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.anno\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.artifact\_1.0.9.jar
- dev/spi/ibm/com.ibm.websphere.appserver.spi.javaeedd\_1.0.9.jar

## Locating OSGi applications

You can use classes in the org.apache.aries.blueprint package to extend the OSGi application programming model; this third-party SPI is provided through the blueprint-1.0 server feature. You must access OSGi application bundles in to apply your extensions. In Liberty, OSGi applications run as Subsystems. To locate an OSGi application you can create a ServiceTracker in a user feature.

## About this task

This topic describes how the developer of a user feature can locate running OSGi applications. This task is often required for user features that provide programming model extensions to OSGi applications. For example, a new user feature might provide such extensions by implementing a new bundle extender, often referred to as a *container*, or, more simply, by tracking and invoking services published from within certain OSGi applications.

Such user features must use the BundleContext of a particular running OSGi application to create new BundleTracker and ServiceTracker instances. This BundleContext can be obtained from the org.osgi.service.subsystem.Subsystem that is associated with the OSGi application. The following procedure describes how to obtain that SubSystem service.

## Procedure

To locate an OSGi application by creating a ServiceTracker in a user feature, complete the following steps:

1. Construct an org.osgi.framework.Filter that is targeted to the Subsystem that you want to locate.
2. Create an org.osgi.util.tracker.ServiceTracker that uses the Filter from step 1 to obtain the org.osgi.service.subsystem.Subsystem service that is associated with the OSGi application that you want to locate. This Subsystem service instance provides everything you require to work with the OSGi application.

## Example

The following example shows how to locate an application with symbolic name `my.app` by using a `ServiceTracker` in a user feature:

```
import org.osgi.framework.BundleContext;
import org.osgi.service.subsystem.Subsystem;
import org.osgi.util.tracker.ServiceTracker;
import org.osgi.util.tracker.ServiceTrackerCustomizer;
```

In the following code extract, the variable `ctx` is the `BundleContext` of one of the bundles of the user feature:

```
String SERVICE_FILTER = "(&(objectClass=org.osgi.service.subsystem.Subsystem)
                        (subsystem.type=osgi.subsystem.application)(subsystem.symbolicName=my.app))"

    org.osgi.framework.Filter filter = ctx.createFilter(SERVICE_FILTER);
```

The last 'null' parameter can be replaced with an instance of a class that implements `ServiceTrackerCustomizer<Subsystem, Subsystem>`:

```
org.osgi.util.tracker.ServiceTracker<Subsystem, Subsystem> str = new ServiceTracker<Subsystem, Subsystem>(ctx, filter, null);
```

The `SERVICE_FILTER` can be constructed to make use of such constants as:

```
org.osgi.framework.Constants.OBJECTCLASS;
org.osgi.service.subsystem.SubsystemConstants.SUBSYSTEM_SYMBOLICNAME_PROPERTY;
org.osgi.service.subsystem.SubsystemConstants.SUBSYSTEM_TYPE_APPLICATION;
org.osgi.service.subsystem.SubsystemConstants.SUBSYSTEM_TYPE_PROPERTY;
```

## Developing with the JNDI default namespace in a Liberty feature

### 8.5.5.0

You can make an object available in the default Java Naming and Directory Interface (JNDI) namespace. To do that, you must register it in the OSGi service registry with the `osgi.jndi.service.name` service property. The value of `osgi.jndi.service.name` is the required JNDI name. Similarly, to find an object in the default JNDI namespace, you can search the OSGi service registry with the `osgi.jndi.service.name` service property. The value of `osgi.jndi.service.name` is the JNDI name.

### About this task

Compared with explicitly calling `Context.bind` or `Context.lookup`, using the service registry has the following benefits:

- Your feature works properly when `jndi-1.0` is enabled, but your feature does not need an explicit dependency on JNDI.
- You do not need to explicitly unbind objects from JNDI when your feature is removed because the OSGi framework automatically unregisters services when bundles are stopped.
- You can easily implement lazy initialization using declarative services or `ServiceFactory` rather than using `Reference` and `ObjectFactory`.

For more information about JNDI, see [Naming](#).

### Procedure

1. Register a service using the `osgi.jndi.service.name` property with the JNDI name. For more information about registering services, see “[Registering OSGi services](#)” on page 1790.
2. Update your `metatype.xml` to allow a JNDI name to be specified in server configuration. To allow users to specify a JNDI name for your service, you should use the `jndiName` id for consistency with other features in the Liberty run time, for example:

```
<AD id="jndiName" name="JNDI name" description="JNDI name for a widget." type="String" ibm:unique="jndiName"/>
```

You can use an internal attribute to automatically set the `osgi.jndi.service.name` service property with the value of the `jndiName` attribute, for example:

```
<AD id="osgi.jndi.service.name" name="internal" description="internal" type="String" default="{jndiName}"/>
```

For more information about OSGi Metatype, see “Advanced Configuration” on page 1798.

3. **8.5.5.1** Implement the `ResourceFactory` interface if you need Java EE resource reference information. If your service needs Java EE resource reference information, such as `res-auth`, you can register a `ResourceFactory` in the OSGi service registry with the `jndiName` and `creates.objectClass` properties. The `ResourceFactory` service is re-registered automatically with the `osgi.jndi.service.name` property. For example:

```
import com.ibm.wsspi.resource.ResourceFactory;
public class WidgetResourceFactory implements ResourceFactory { ... }

Properties properties = new Properties();
properties.put(ResourceFactory.JNDI_NAME, "widget/abc");
properties.put(ResourceFactory.CREATE_OBJECT_CLASS, Widget.class.getName());
bundleContext.registerService(ResourceFactory.class, new WidgetResourceFactory(), properties);
```

Alternatively, the service could be registered automatically using declarative services and metatype. In that case, you can specify the `creates.objectClass` property as a declarative services property. You do not need to specify the `jndiName` property because it is set automatically from the user configuration with the `<AD id="jndiName">` element in the `metatype.xml` file in step 2 on page 1819, and you do not need an `<AD id="osgi.jndi.service.name">` element in the `metatype.xml` file because the `ResourceFactory` service will be re-registered automatically.

4. Locate an object using the `osgi.jndi.service.name` property with the JNDI name. For example:  
`bundleContext.getServiceReference(DataSource.class, "(osgi.jndi.service.name=jdbc/myds)");`

**8.5.5.0** Alternatively, you can locate a `ResourceFactory` using the `jndiName` and `creates.objectClass` properties.

5. Update your `metatype.xml` to allow a resource to be specified in `server.xml` using the id of the resource. This allows the resource to be accessed regardless of whether or not the resource has a `jndiName`. For example,

```
<AD id="dataSourceRef" type="String" ibm:type="pid" ibm:reference="com.ibm.ws.jdbc.dataSource" cardinality="1" name="%d
```

If you are using declarative services, you can use an internal attribute to set a `.target` service property with a filter. For example, if your declarative services component has a reference named `dataSource`, you can use the following attribute definition to ensure that the `dataSource` that is referenced by the `dataSourceRef` configuration attribute is used.

```
<AD id="dataSource.target" type="String" default="(service.pid={dataSourceRef})" ibm:final="true" name="internal" desc
```

## Developing a custom TAI as a Liberty feature

### 8.5.5.0

You can develop a custom TAI as a Liberty feature by implementing the `com.ibm.wsspi.security.tai.TrustAssociationInterceptor` interface provided in the Liberty server and creating a product extension.

### About this task

For a general view of custom TAI, see “Developing a custom TAI for Liberty” on page 1998.

For more information about product extensions, see “Liberty profile: Product extension” on page 967.

**Avoid trouble:** If you have multiple TAIs, you can configure all of them by using either the user feature or the shared library. Do not mix the two TAI configurations.

## Procedure

1. Implement the custom TAI. For more information, see “Developing a custom TAI for Liberty” on page 1998.
2. Convert the implementation class into an OSGi service. You can do the conversion in one of the following ways:
  - Convert your custom TAI class into a Declarative Service (DS) component. For more information, see “Declaring your services to OSGi Declarative Services” on page 1794.
  - Write a new custom TAI class that is a DS component and delegate it to your custom TAI class.
  - Register the custom TAI class directly in the Service Registry (SR) by using the OSGi core APIs. For more information, see “Working with the OSGi service registry” on page 1789.
3. Package the custom TAI as an OSGi bundle and export the custom TAI service. For information on creating an OSGi bundle, see *Creating an OSGi service bundle*.
4. Create a feature manifest to include the OSGi bundle. For more information about feature manifest file, see “Liberty feature manifest files” on page 1773.
5. After the feature is installed into the user product extension location, configure the `server.xml` file with the feature name. For example:

```
<featureManager>
  ...
  <feature>usr:customTaiSample-1.0</feature>
</featureManager>
```

## Dynamic content management

You typically install bundles into the runtime environment by listing them in the `Subsystem-Content` header of the feature manifest file. However, you can also dynamically add and remove OSGi bundles by installing a user-written bundle as part of the `Subsystem-Content` of a user-written feature. The user-written bundle obtains the OSGi bundle context to install and control additional bundles.

## Installing, starting, stopping, and uninstalling bundles in Liberty

**Note:** In the following sections, the user-written feature is called `UserFeatureA` and the user-written bundle is called `FeatureBundleA`.

### Installing bundles

You can write `FeatureBundleA` to obtain the OSGi bundle context, `org.osgi.framework.BundleContext`, by using one of the following methods:

- Implement the `BundleActivator` interface, `org.osgi.framework.BundleActivator`. The `BundleContext` parameter of the `start` method is passed in by the OSGi framework, which is available to the user-written bundle when that bundle is activated. For more information on the `BundleActivator` interface, see “Developing an OSGi bundle with simple activation” on page 1788.
- Implement an available specification, such as OSGi Declarative Services or Blueprint, that provides access to the bundle context through another method or interface. For more information, see “Composing advanced features by using OSGi Declarative Services” on page 1793 and *Blueprint bundles*.

After `FeatureBundleA` obtains the bundle context, additional bundles can be installed by using either the `installBundle(String location)` or `installBundle(String location, InputStream stream)` methods.

Bundles that are dynamically installed resume state on a default restart. They do not persist across a clean start and require reinstallation. See *Bundle caching* for more details.

## Starting bundles

If you want an installed bundle to be started, it is the responsibility of the installing bundle, `FeatureBundleA`, to call the `start` method for the bundle.

## Stopping and uninstalling bundles

If the user-written feature, `UserFeatureA`, is removed from the server configuration, then `FeatureBundleA` is stopped and also uninstalled. Uninstallation of `FeatureBundleA` triggers uninstallation of all the bundles that were installed by `FeatureBundleA`, if they are not already uninstalled. The `org.osgi.framework.Bundle.uninstall()` method is called for each bundle, which stops and uninstalls it. This uninstallation process also applies if `FeatureBundleA` is uninstalled by any other means.

If `UserFeatureA` is removed from the server configuration when the server is stopped, the bundles that were installed by `UserFeatureA` are removed on the next server start. If the start levels of the bundles are unmodified from their defaults, the bundles are removed before they are restarted. If the start levels of the bundles were modified, they might not be removed until after they have restarted.

Other lifecycle management tasks are done by `FeatureBundleA` according to the OSGi core specification, by using the `org.osgi.framework.Bundle` and `org.osgi.framework.BundleContext` interfaces.

## Bundle caching, package visibility, and programming model support in Liberty

### Bundle caching

When the server is shut down, all the currently installed bundles are stopped and OSGi metadata is persisted to a bundle cache. On a default start, these installed bundles are returned to their previous state. On a clean start, any bundles that were installed by `FeatureBundleA` have their persistent data deleted. As a result, on a clean start these bundles are not resumed.

`FeatureBundleA` itself is resumed because it is reinstalled by the feature manager, provided `UserFeatureA` is still in the server configuration. If you want to reinstall any bundles after a clean start, it is the responsibility of `FeatureBundleA` to do the reinstallation. You are not notified about a clean start, but you can check whether a bundle is installed by using the OSGi `BundleContext` `getBundle(String location)` method.

### Package visibility

Bundles that are dynamically installed, and are not listed in the `Subsystem-Content` header of the feature manifest file, have the following visibility:

- Dynamically installed bundles can import any API and SPI packages provided by the currently configured set of features.
- Packages that are exported by other bundles within the same product extension that are not declared as API or SPI, are not visible to dynamically installed bundles.
- Packages that are exported from dynamically installed bundles cannot be declared as API or SPI.
- There are no restrictions on importing packages that are exported from dynamically installed bundles.

### Programming model support

Dynamically installed bundles can use implementations of OSGi enterprise specifications provided that the appropriate runtime features are configured to enable them.

---

## Packaging and installing Liberty features

8.5.5.0

You can package and install Liberty features to WebSphere Application Server Liberty.

## About this task

A Liberty feature may be packaged as a subsystem archive, as defined by the OSGi Enterprise specification (5.0). A subsystem archive is a compressed file with an `.esa` extension that includes the feature manifest and the resource files that constitute the feature. The WebSphere Application Server developer tools will import and export Liberty features by using the subsystem archive format, and features can be installed to a Liberty runtime environment by using the **featureManager** command if they are in the `.esa` format.

## Procedure

- You can manually install a Liberty features onto Liberty.
  - To install the feature to the Liberty kernel, the feature manifest file must be in the `${wlp.install.dir}/lib/features` directory and related bundles in the `${wlp.install.dir}/lib` directory;
  - To install the feature into the user configuration, the feature manifest file must be in the `${wlp.user.dir}/extension/lib/features` directory, and related bundles must be in the `${wlp.user.dir}/extension/lib` directory;
  - To install the feature into a product extension, the feature manifest file and related bundles must be in the product extension directory. The product extension is registered in the `${wlp.user.dir}/etc/extension/lib/features` directory using a `<extension-name>.properties` file. For more information, see “Liberty profile: Product extension” on page 967.
- You can also use the **featureManager** command that is provided in the `${wlp.install.dir}/bin` directory to install a Liberty feature if it is packaged as an `.esa` file.
  - To install a feature as a user feature, use the following command:  

```
featureManager install my_feature.esa --to=usr
```
  - To install a feature to a product extension location, use the following command:  

```
featureManager install my_feature.esa --to=my_extension
```

For more information about the **featureManager** command, see “Liberty:featureManager command” on page 1405.

## Provide product information for your feature extension

**8.5.5.0**

You can provide Version Product information for your Feature Extension

You can provide Version Product information for your Feature Extensions by providing the installation with a uniquely named product information properties file in the `lib/versions` directory of the extension. The file extension must be `.properties`.

You can add Version Product information manually or by using the **featureManager** script's installation option under the following conditions:

- The subsystem manifest file in the feature archive contains a `subsystem-content` entry that points to the product information properties file that is being installed.
- The product information properties file can be installed only if the feature that is being installed defines the **IBM-Feature-Version**.
- The product information properties file in the feature archive (`.esa`) has the following path  
`wlp/lib/versions/filename.properties`.

The following properties can be specified in the product information properties file:

```
com.ibm.websphere.productId=yourProductID
com.ibm.websphere.productOwner=TheProductOwner
com.ibm.websphere.productVersion=yourProductVersion
```

```
com.ibm.websphere.productName=yourProductName
com.ibm.websphere.productInstallType=yourProductInstallType
com.ibm.websphere.productEdition=yourProductEdition
com.ibm.websphere.productQualifier=yourProductQualifier
```

If you want to override a particular feature extension information, include the following property in your product information properties file:

```
com.ibm.websphere.productReplaces=theProductIdToReplace
```

If your product is eligible for Getting Started Subcapacity Pricing (GSSP), set the following property to true in your product information properties file:

```
com.ibm.websphere.gssp=true
```

The following is an example of how to define subsystem entry content for installing the feature extension by using the featureManager script, subsystem.mf:

```
Subsystem-ManifestVersion:1
...
Subsystem-Content: userProdExt; version="[1,1.0.100]",
user.ext.version.info; type="file"; location:="lib/versions/user.ext.version.info.properties"
IBM-Feature-Version: 2
```

The following is an example that shows the output of the *productInfo* script using the *version* option that shows the product name and version entries that are specified in the product information properties file:

```
com.ibm.websphere.productId=XYZ Product ID
com.ibm.websphere.productOwner=XYZ Inc
com.ibm.websphere.productVersion=1.0.0
com.ibm.websphere.productName=XYZ User Product
com.ibm.websphere.productInstallType=Archive
com.ibm.websphere.productEdition=Enterprise Edition
```

```
Command:
productInfo version
```

```
Output:
Product name: Websphere Application Server
Product version: 8.5.5.0
```

```
Product name: XYZ User Product
Product version: 1.0.0
```

---

## Embedding Liberty in your applications

**8.5.5.0**

You can use the System Programming Interfaces (SPIs) that are provided by Liberty to configure, control, and monitor a Liberty server in your applications.

### About this task

Liberty provides the following SPIs to start or stop a Liberty server:

- `com.ibm.wsspi.kernel.embeddable.Server`
- `com.ibm.wsspi.kernel.embeddable.ServerBuilder`

Use a Future object to store the result of a start or stop operation. The return codes that are used by embedded operations are the same as the return codes used by the **server** command. For more information about return codes, JVM options used by the server script, and the process environment used by the server script, see “Liberty:server command options” on page 1569.

Additionally, you can receive asynchronous notifications when the server is starting, has started, or has stopped by creating your own class that implements the `com.ibm.wsspi.kernel.embeddable.ServerEventListener` interface.

**Note:** To create an instance of an embedded server within your application, you must carry out the following steps:

- Include the `ws-server.jar` file on the class path. The `ws-server.jar` file is in the `${wlp.install.dir}/bin/tools` directory of the Liberty installation.
- Specify the name of the target server. The target server must exist.
- Optional: Configure the `ws-javaagent.jar` file with the `-javaagent` JVM option. The `ws-javaagent.jar` file is in the `${wlp.install.dir}/bin/tools` directory of the Liberty installation. You are advised to configure the `ws-javaagent.jar` file, but it is not mandatory unless you use capabilities of the server that require it, such as monitoring or trace. If you contact IBM support, you might need to provide trace, and if so, you must start the server with the `ws-javaagent.jar` file, even if you do not normally use it.

**Note:** In an embedded environment:

- Environment variables are not checked, and the `jvm.options` and `server.env` files are not read.
- Management of the JVM and environment is assumed to be managed by the caller.

## Procedure

1. Import the SPIs into your caller class and define the arguments that are required to operate the Liberty server.

```
import com.ibm.wsspi.kernel.embeddable.Server;
import com.ibm.wsspi.kernel.embeddable.ServerBuilder;

public class MyEmbeddedServer {
    String serverName="defaultServer";
    File userDir = new File("usr");
    File outputDir = new File("usr/servers/");
    ...
}
```

Where

- The **serverName** is required, and must match the name of a previously created server.
  - The **userDir** is optional and used to set the path of the user directory. By default, the user directory is `${wlp.user.dir}`.
  - The **outputDir** is optional and used to set the path of the output directory. By default, the output directory is `${wlp.user.dir}/servers`.
2. Initialize the server by using the `ServerBuilder` class.

```
ServerBuilder sb = new ServerBuilder();
Server libertyServer = sb.setName(serverName)
                        .setUserDir(userDir)
                        .setOutputDir(outputDir)
                        .build();
```
  3. Call the `Server.start()` method to start the server. Call `get()` on the future to block until the start operation completes. Use one of the following to determine whether the server started successfully:
    - Check the returned result code.
    - Use the `successful()` method.
    - If the server is started, the `server.isRunning()` method returns true.

```
Future<Result> startReturnCode = libertyServer.start();
Result result = startReturnCode.get(); // block until operation complete, if necessary
System.out.println("Start returned: success=" + result.successful() + ", rc=" + result.getReturnCode() + ", ex=" + result.getException());
```

4. Call the `Server.stop()` method to stop the server. Call `get()` on the future to block until the stop operation completes. Use one of the following to determine whether the server stopped successfully:
  - Check the returned result code.
  - Use the `successful()` method.
  - If the server is stopped, the `server.isRunning()` method returns false.

```
Future<Result> stopReturnCode = libertyServer.stop();
Result result = stopReturnCode.get(); // block until operation complete, if necessary
System.out.println("Stop returned: success=" + result.successful() + ", rc=" + result.getReturnCode() + ", ex=" + result.getException());
```

5. Implement the `ServerEventListener` interface. If you implement the `ServerEventListener` interface, you can receive notifications when the server is started or stopped.

```
// update the class declaration to indicate that it implements ServerEventListener
public class MyEmbeddedServer implements ServerEventListener {
    ...
    MyEmbeddedServer() throws ServerException {
        // set the listener via the server builder
        ServerBuilder sb = new ServerBuilder();
        Server libertyServer = sb.setName(serverName)
                                .setServerEventListener(this)
                                .build();
    }

    ...
    @Override
    public void serverEvent(ServerEvent event) {
        // provide an implementation of the serverEvent method
        System.out.println("serverEvent: " + event);
    }
}
```

---

## Creating Liberty servers from custom configurations

### 8.5.5.0

You can create a server from a custom configuration for any environment that you require.

### About this task

The Liberty server script `create` command offers a `--template` option. You can use this option to support server creation from a custom configuration located within a `templates/servers/<template-name>` sub-directory of your product extension. Custom server templates must contain at least a `server.xml` file, and can contain any configuration files, for example: `bootstrap.properties` or `jvm.options`.

### Procedure

You can use the `--template` option in the following way: `server create --template=<extension-name>:<template-name>`

---

## Disabling z/OS operator console command handling in the Liberty server

z/OS

### 8.5.5.2

You can listen for and handle z/OS operator console commands directly from your application or product extension feature. However, doing so conflicts with the built-in Liberty for z/OS operator console command handler. If you want to listen for commands directly, you need to disable the built-in Liberty for z/OS operator console command listener.

## About this task

Liberty provides the following property to disable the handling of z/OS operator console commands by the Liberty server:

```
websphere.os.extension=zosNoConsoleExtensions-1.0
```

## Procedure

1. Stop the Liberty server.
2. Set `websphere.os.extension=zosNoConsoleExtensions-1.0` in your `${server.config.dir}/bootstrap.properties` file.
3. Start the Liberty server.

When you start the Liberty server with this new setting, it no longer listens for z/OS console commands. This change allows your application to handle z/OS console commands itself. For more information on implementing z/OS console command listeners and handlers within an application, see *MVS Programming Authorized Assembler Services Guide: Communicating with a program (EXTRACT, QEDIT)*, or the equivalent for your level of z/OS.



---

## Chapter 8. Securing Liberty and its applications

This information applies to all types of applications that are deployed on Liberty.

### About this task

Security in Liberty supports all the Servlet 3.0 security features and secured Java JMX connections. The following Liberty features are applicable to security in Liberty:

- `appSecurity-2.0` enables security for **8.5.5.0** for web applications when the `servlet-3.0` feature is present and for EJB components when the `ejbLite-3.1` feature is present.
- `ssl-1.0` enables SSL connections using HTTPS.
- **z/OS** `zosSecurity-1.0` includes the support for SAF Registry and Authorization on the z/OS platform.
- `restConnector-1.0` enables remote access by JMX client through a REST-based connector.
- `oauth-2.0` enables authorization to resources by using the OAuth 2.0 protocol.
- **8.5.5.0** `ldapRegistry-3.0` provides support for the LDAP user registry.

To learn about how security works in Liberty, see “Liberty: Security” on page 971.

**Best practice:** **8.5.5.0** There are several security configuration examples on the `WASdev.net` website for reference when configuring security for your applications on Liberty. If you see any differences in the configuration created by the developer tools and the examples, modify the configuration to fit the configuration in the examples for that feature.

### Procedure

- Use `quickStartSecurity` for minimal security configuration
- Secure communications in Liberty
- Access a secured JMX connector in Liberty
- Authenticate users in Liberty
- Authorize access to resources in Liberty
- Secure a database access application
- Develop extensions to the Liberty security infrastructure

---

## Getting started with security in Liberty

You can use the `<quickStartSecurity>` element to quickly enable a simple (one user) security setup for Liberty.

### About this task

You can set up a secured Liberty server and web application by following some basic configuration steps. Configuration actions within Liberty are dynamic, which means the configuration updates take effect without having to restart the server.

### Procedure

1. Create and start your server.
  - **Windows** On Windows systems:

```
server.bat create MyNewServer
server.bat start MyNewServer
```

- **AIX** **Linux** **UNIX** **HP-UX** **Solaris** **IBM i** **z/OS** On all systems other than Windows systems:

```
server create MyNewServer
server start MyNewServer
```

2. **8.5.5.0** Include the appSecurity-2.0 and servlet-3.0 features in the server.xml file. The server.xml file is in the server directory of *myNewServer*, for example, wlp\usr\servers\myNewServer\server.xml.

```
<featureManager>
  <feature>appSecurity-2.0</feature>
  <feature>servlet-3.0</feature>
</featureManager>
```

3. Define the user name and password that is to be granted the Administrator role for server management activities.

```
<quickStartSecurity userName="Bob" userPassword="bobpwd" />
```

**Note:** Choose a user name and password that are meaningful to you. Never use the name and password in the example for your applications.

4. Configure the deployment descriptor with relevant security constraints to protect web resource. For example, use <auth-constraint> and <role-name> elements to define a role that can access web resource.

The following example web.xml file shows that access to all the URIs in the application is protected by the testing role.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
    "http://java.sun.com/dtd/web-app_2_3.dtd">
```

```
<web-app id="myWebApp">

  <!-- SERVLET DEFINITIONS -->
  <servlet id="Default">
    <servlet-name>myWebApp</servlet-name>
    <servlet-class>com.web.app.MyWebAppServlet</servlet-class>
    <load-on-startup/>
  </servlet>

  <!-- SERVLET MAPPINGS -->
  <servlet-mapping id="ServletMapping_Default">
    <servlet-name>myWebApp</servlet-name>
    <url-pattern>/*</url-pattern>
  </servlet-mapping>

  <!-- SECURITY ROLES -->
  <security-role>
    <role-name>testing</role-name>
  </security-role>

  <!-- SECURITY CONSTRAINTS -->
  <security-constraint>
    <web-resource-collection>
      <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <role-name>testing</role-name>
    </auth-constraint>
  </security-constraint>

  <!-- AUTHENTICATION METHOD: Basic authentication -->
```

```

<login-config>
  <auth-method>BASIC</auth-method>
</login-config>

</web-app>

```

5. Configure your application in the `server.xml` file.

In the following example, the user Bob is mapped to the testing role of the application:

```

<application type="war" id="myWebApp" name="myWebApp"
  location="${server.config.dir}/apps/myWebApp.war">
  <application-bnd>
    <security-role name="testing">
      <user name="Bob" />
    </security-role>
  </application-bnd>
</application>

```

6. Access your application and log in with the user name Bob. The default URL for the myWebApp application is `http://localhost:9080/myWebApp`

## Results

You have now secured your application.

## Liberty:Quick overview of security

To understand the basic workflow of security in Liberty, some common security terms are detailed along with an example.

### Security key terms

#### Authentication

Authentication confirms the identity of a user. The most common form of authentication is user name and password, such as through basic authentication or form login for web applications. When a user is authenticated, the source of a request is represented as a Subject object at run time.

#### Authorization

Authorization determines whether a user has access to a given role within the system. The Java EE model uses subjects, roles, and role mappings to determine if access is allowed.

**Role** A role is defined within the Java EE application. Some roles, such as the Administrator role, are predefined by the system. Other roles are defined by the application developer. In Java EE, subjects are usually granted or denied access to a role based on the roles they perform within the application.

#### Subject

A subject is both a general term and a Java object: `javax.security.auth.Subject`. Generally, the term subject means active entities within the system, such as users on the system, and even the system process itself.

### Security workflow example

The following example demonstrates how the security is applied when a user requests access to a resource. For example, a user Bob wants to access a servlet myWebApp. See the code samples in “Getting started with security in Liberty” on page 1829.

To access the servlet myWebApp, the following conditions must be true:

1. Bob must be able to log in to the system because the servlet is protected.
2. Bob must be in the testing role because the servlet is restricted by using an `auth-constraint` element in the deployment descriptor.

If Bob cannot log in to the system, or Bob is not in the testing role, then the access to the servlet myWebApp is denied.

Another user Alice can log in to the system because Alice is a valid user. But Alice is not in the testing role. An HTTP 403 error (Access Denied/Forbidden) displays when Alice logs in.

## Setting up BasicRegistry and role mapping on Liberty

You can configure Liberty to authenticate and authorize users by using a basic user registry.

### Before you begin

**8.5.5.0** The Liberty features appSecurity-2.0 and servlet-3.0 must be enabled in the server.xml file.

For more information about security configuration in Liberty, see “Getting started with security in Liberty” on page 1829.

### About this task

You can set up a basic user registry and configure more role mapping in the server.xml file for a Liberty server by going through the following steps.

### Procedure

1. Configure the basic registry as follows. Use a user name and password that are meaningful to you. Never use the name and password from this example in your applications.

```
<basicRegistry id="basic" realm="WebRealm">
  <user name="Bob" password="bobpwd" />
</basicRegistry>
```

2. Optional: Grant the user or group the Administrator role if the user, or group of users, is used to perform remote system management activities. This step is done automatically when using the quickStartSecurity element or may be accomplished by adding the administrator-role element to the server.xml file as shown.

```
<administrator-role>
  <user>Bob</user>
  <group>myAdmins</group>
</administrator-role>
```

3. Encode the password within the configuration. You can get the encoded value by using the securityUtility encode task.
4. Optional: Add additional users. Make sure that each user name is unique.

```
<basicRegistry id="basic" realm="WebRealm">
  <user name="Bob" password="bobpwd" />
  <user name="user1" password="user1pwd" />
  <user name="user2" password="user2pwd" />
</basicRegistry>
```

5. Create groups for users. Make sure that each group name must be unique.

```
<basicRegistry id="basic" realm="WebRealm">
  <user name="Bob" password="bobpwd" />
  <user name="user1" password="user1pwd" />
  <user name="user2" password="user2pwd" />

  <group name="myAdmins">
    <member name="Bob" />
    <member name="user1" />
  </group>

  <group name="users">
```

```

        <member name="user1" />
        <member name="user2" />
    </group>
</basicRegistry>

```

6. Assign some users and groups to the testing role of an application.

```

<application type="war" id="myWebApp" name="myWebApp"
    location="{server.config.dir}/apps/myWebApp.war">
    <application-bnd>
        <security-role name="testing">
            <user name="Bob" />
            <user name="user1" />
            <group name="users" />
        </security-role>
    </application-bnd>
</application>

```

## What to do next

Configure security-related elements in the deployment descriptor of your application. See “Getting started with security in Liberty” on page 1829 for a sample `web.xml` file.

---

## Securing communications in Liberty

You can configure the Liberty server to provide secure communications between a client and the server.

### About this task

Communications are secured with Secure Sockets Layer (SSL) protocol. The SSL protocol provides transport layer security including authenticity, data signing, and data encryption to ensure a secure connection between a client and server that uses WebSphere® Application Server. The foundation technology for SSL is public key cryptography, which guarantees that when an entity encrypts data using its public key, only entities with the corresponding private key can decrypt that data. The Liberty Server uses Java Secure Sockets Extension (JSSE) as the SSL implementation for secure connections. JSSE handles the handshake negotiation and protection capabilities that are provided by SSL to ensure that secure connectivity exists across most protocols. JSSE relies on X.509 certificate-based asymmetric key pairs for secure connection protection and some data encryption. Key pairs effectively encrypt session-based secret keys that encrypt larger blocks of data. The SSL implementation manages the X.509 certificates.

To configure secure communications, you can either specify a minimal SSL configuration or a detailed SSL configuration in the `server.xml` file. The minimal configuration only requires the SSL feature and a keystore entry to be specified. **8.5.5.0** There are several security configuration examples on the `WASdev.net` website for reference when configuring security for your applications on Liberty.

**8.5.0.1** The SSL configuration that is designated as the default SSL configuration is used to create the process's default `SSLContext` using the `SSLContext.setDefault()` method. The default SSL configuration can be the minimal SSL configuration, or the configuration that is identified by the `sslRef` attribute on the `sslDefault` element if multiple SSL configurations are defined. Because the default `SSLContext` is set on the process, the `javax.net.ssl.keyStore` and `javax.net.ssl.trustStore` properties will not be recognized.

### Procedure

- Enable SSL communications between a client and a Liberty server
- Optional: Create a keystore from the command prompt
- Optional: Encode passwords from the command prompt
- Optional: Configure client certificate authentication between your application and the Liberty server

## Enabling SSL communication in Liberty

To enable SSL communication in Liberty, there is a minimal set of SSL configuration options. It assumes most of the SSL options require some keystore configuration information.

### About this task

SSL client authentication occurs during the connection handshake by using SSL certificates. The SSL handshake is a series of messages that are exchanged over the SSL protocol to negotiate for connection-specific protection. During the handshake, the secure server requests that the client send back a certificate or certificate chain for the authentication. To enable SSL in Liberty, you add the `ssl-1.0` Liberty feature to the configuration root document file, `server.xml`, along with code of the keystore information for authentication.

By default, the path and file name for the configuration root document file is `path_to_liberty/wlp/usr/servers/server_name/server.xml`. `path_to_liberty` is the location that you installed Liberty on your operating system, and `server_name` is the name of your server. However, you can change the path. See “Customizing the Liberty environment” on page 1565.

### Procedure

1. Enable the `ssl-1.0` Liberty feature in the `server.xml` file.

```
<featureManager>
  <feature>ssl-1.0</feature>
</featureManager>
```

**Note:** If application security is required and security information is redirected to a secure port, you must add the `appSecurity-2.0` Liberty feature to the `server.xml` file.

2. Add the keystore service object entry to the `server.xml` file. The `keyStore` element is called `defaultKeyStore` and contains the keystore password. The password can be entered in clear text or encoded. The `securityUtility encode` option can be used to encode the password.

```
<keyStore id="defaultKeyStore" password="yourPassword" />
```

This configuration is the minimum that is needed to create an SSL configuration. In this configuration, the server creates the keystore and certificate if it does not exist during SSL initialization. The password that is provided must be at least 6 characters long. The keystore is assumed to be a JKS keystore that is called `key.jks` in the server `home/resources/security` directory. If the file does not exist the server creates it for you. If the server creates the keystore file, it also creates the certificate inside of it. The certificate is a self-signed certificate with a validity period of 365 days, the CN value of the certificate's subjectDN is the host name of the machine where the server is running, and has a signature algorithm of `SHA256withRSA`.

**Note:** When the use of a collective controller is not practical, perhaps there is only one or two Liberty servers, a self-signed certificate can be used to restrict the number of clients that can connect to the Liberty member server. It is suggested that an IHS server is used in front of the Liberty servers, where an appropriate CA signed certificate can be used, along with CN whitelisting to control which clients can connect to HIS. A trusted channel between IHS and the Liberty member server can be maintained by using the self signed certificate.

An example of a SAF keyring in the minimal configuration:

```
<keyStore id="defaultKeyStore" location="safkeyring:///WASKeyring"
  type="JCERACFKS" password="password" fileBased="false"
  readOnly="true" />
```

RACF keyring needs to be set up before you configure them for use by the Liberty server. The server does not create certificates and add them to RACF.

The single keystore entry for a minimal SSL configuration can be extended to include the location and type as well.

```
<keyStore id="defaultKeyStore" location="myKeyStore.p12" password="yourPassword" type="PKCS12"/>
```

The **location** parameter can be an absolute path to the keystore file. If it is an absolute path, then the keystore file is assumed to have been already created. Keystore of other types can also be specified in the minimal SSL configuration if the keystore file is already created. When the minimal SSL configuration is used, the SSL configuration defaults are used to create the SSL context for an SSL handshake. The configuration protocol is `SSL_TLS` by default. The HIGH ciphers, 128 bit, and higher cipher suites can be used.

## Liberty:SSL configuration attributes

SSL configurations contain attributes that you use to control the behavior of the server SSL transport layer on Liberty. This topic iterates all the settings available for an SSL configuration.

### SSL Feature

To enable SSL on a server, the SSL feature must be included in the `server.xml` file:

```
<featureManager>
  <feature>ssl-1.0</feature>
</featureManager>
```

### SSL Default

You can have multiple SSL configurations configured. If more than one SSL configuration is configured, then the default SSL configuration must be specified in the `server.xml` file that uses the `sslDefault` service configuration.

*Table 127. Attribute of the `sslDefault` element.* This table describes the attribute of the `sslDefault` element.

Attribute	Description	Default Value
<b>sslRef</b>	The <code>sslRef</code> attribute specifies the name of the SSL configuration to be used as the default.	The default SSL Configuration name is <code>defaultSSLConfig</code> .

In the `server.xml` file, the entry is as follows:

```
<sslDefault sslRef="mySSLSettings" />
```

### SSL Configuration

You use the SSL configuration attributes to customize the SSL environment to suit your needs. These attributes can be set on the `ssl` service configuration element in the `server.xml` file.

*Table 128. Attributes of the `SSL` element.* This table describes the attributes of the `ssl` element.

Attribute	Description	Default Value
<b>id</b>	The <code>id</code> attribute assigns a unique name to the SSL configuration object.	No default value; a unique name must be specified.
<b>keyStoreRef</b>	The <code>keyStoreRef</code> attribute names the keystore service object that defines the SSL configurations keystore. The keystore holds the key that is required to make an SSL connection.	No default value; a keystore reference must be specified.
<b>trustStoreRef</b>	The <code>trustStoreRef</code> attribute names the keystore service object that defines the SSL configurations truststore. The truststore holds certificates that are required for signing verification.	<code>trustStoreRef</code> is an optional attribute. If the reference is missing, the keystore that is specified by <code>keyStoreRef</code> is used.

Table 128. Attributes of the SSL element (continued). This table describes the attributes of the ssl element.

Attribute	Description	Default Value
<b>clientAuthentication</b>	The <b>clientAuthentication</b> attribute determines whether SSL client authentication is required.	Default value is <b>false</b> .
<b>clientAuthenticationSupported</b>	The <b>clientAuthenticationSupported</b> attribute determines whether SSL client authentication is supported. The client does not have to supply a client certificate. If the <b>clientAuthentication</b> attribute is set to true, the value of the <b>clientAuthenticationSupported</b> attribute is overwritten.	Default value is <b>false</b> .
<b>sslProtocol</b>	The <b>sslProtocol</b> attribute defines the SSL handshake protocol. The protocol can be SDK-dependent, so if you modify the protocol make sure that the value is supported by the SDK you are running under.	Default value is <b>SSL_TLS</b> .
<b>securityLevel</b>	The <b>securityLevel</b> attribute determines the cipher suite group to be used by the SSL handshake. The attribute has one of the following values: <ul style="list-style-type: none"> <li>• <b>HIGH</b> (128-bit ciphers and higher)</li> <li>• <b>MEDIUM</b> (40-bit ciphers)</li> <li>• <b>WEAK</b> (for all ciphers without encryption)</li> <li>• <b>CUSTOM</b> (if the cipher suite group is customized).</li> </ul> When you set the <b>enabledCiphers</b> attribute with a specific list of ciphers, the system ignores this attribute.	Default value is <b>HIGH</b> .
<b>enabledCiphers</b>	The <b>enabledCiphers</b> attribute is used to specify a unique list of cipher suites. Separate each cipher suite in the list with a space. If the <b>enabledCiphers</b> attribute is set, then the <b>securityLevel</b> attribute is ignored.	No default value.
<b>serverKeyAlias</b>	The <b>serverKeyAlias</b> attribute names the key in the keystore to be used as the SSL configurations key. This attribute is only required if the keystore has more than one key entry in it. If the keystore has more than one key entry and this attribute does not specify a key, then the JSSE picks a key.	No default value.
<b>clientKeyAlias</b>	The <b>clientKeyAlias</b> attribute names the key in the keystore to be used as the key for SSL configuration when <b>clientAuthentication</b> is enabled. The attribute is only required if the keystore contains more than 1 key entry.	No default value.

Note:

- The key manager is used by the SSL handshake to determine what certificate alias to use. The key manager is not configured in the `server.xml` file. It is retrieved from the security property `ssl.KeyManagerFactory.algorithm` of the SDK.
- The trust manager is used by the SSL handshake to make trust decisions. The trust manager is not configured in the `server.xml` file. It is retrieved from the security property `ssl.TrustManagerFactory.algorithm` of the SDK.

Here is an example of how the `ssl` element is configured in the `server.xml` file:

```
<!-- Simple ssl configuration service object. This assumes there is a keystore object named -->
<!-- defaultKeyStore and a truststore object named defaultTrustStore in the server.xml file. -->
  <ssl id="myDefaultSSLConfig"
      keyStoreRef="defaultKeyStore"
      trustStoreRef="defaultTrustStore" />
```

```
<!-- A ssl configuration service object that enabled clientAuthentication -->
<!-- and specifies the TLS protocol be used. -->
  <ssl id="myDefaultSSLConfig"
      keyStoreRef="defaultKeyStore"
      trustStoreRef="defaultTrustStore"
      clientAuthentication="true"
      sslProtocol="TLS" />
```

```
<!-- An SSL configuration service object that names the serverKeyAlias -->
<!-- to be used by the handshake. This assumes there is a certificate -->
<!-- called "default" in the keystore defined by keyStoreRef. -->
  <ssl id="myDefaultSSLConfig"
      keyStoreRef="defaultKeyStore"
      serverKeyAlias="default" />
```

## Keystore Configuration

The keystore configuration consists of the attributes that are required to load a keystore. These attributes can be set on the keystore service configuration in the `server.xml` file.

*Table 129. Attributes of the keystore element.* This table explains the attributes of the keystore element.

Attribute	Description	Default Value
<b>id</b>	The <b>id</b> attribute defines a unique identifier of the keystore object.	No default value, a unique name must be specified.
<b>location</b>	The <b>location</b> attribute specifies the keystore file name. The value can include the absolute path to the file. If the absolute path is not provided, then the code looks for the file in the <code>\${server.config.dir}/resources/security</code> directory.	In the SSL minimal configuration, the location of the file is assumed to be <code>\${server.config.dir}/resources/security/key.jks</code> .
<b>type</b>	The <b>type</b> attribute specifies the type of the keystore. Check that the keystore type that you specify is supported by the SDK you are running on.	Default value is <b>jks</b> .

Table 129. Attributes of the keystore element (continued). This table explains the attributes of the keystore element.

Attribute	Description	Default Value
<b>password</b>	The <b>password</b> attribute specifies the password that is used to load the keystore file. The password can be stored either in clear text or encoded. For information about how to encode the password, see the securityUtility encode option.	Must be provided.
<b>provider</b>	The <b>provider</b> attribute specifies the provider to be used to load the keystore. Some keystore types required a provider other than the SDK default.	By default no provider is specified.
<b>fileBased</b>	The <b>fileBased</b> attribute specifies whether the keystore is file-based.	Default value is <b>true</b> .
<b>pollingRate</b>	The rate at which the server checks for updates to a keystore file.	<b>500ms</b> .
<b>updateTrigger</b>	The method that is used to trigger the server to reload a keystore file. Specify <b>polled</b> to enable the server for checking the keystore file for changes, <b>mbean</b> to enable the server to wait for an mbean to reload the keystore file, or <b>disabled</b> to disable file monitoring.	<b>disabled</b> .

Keystore files can be reloaded by the server if the **updateTrigger** attribute is set to **polled** or **mbean**. If **polled** is enabled, then the server monitors the keystore file for changes based on the rate set in the **pollingRate** attribute. If the **updateTrigger** attribute is set to **mbean** then the server will reload the keystore file when it receives notification from the `WebSphere:service=com.ibm.ws.kernel.filemonitor.FileNotificationMBean` MBean. File monitoring is disabled by default.

Here is an example of how the keystore element is configured in the `server.xml` file:

```
<!-- A keystore object called defaultKeyStore provides a location, -->
<!-- type, and password. The MyKeyStoreFile.jks file is assumed -->
<!-- to be located in ${server.config.dir}/resources/security -->
<!-- This keystore is configured to be monitored every 5 seconds -->
<!-- for updates -->
  <keyStore id="defaultKeyStore"
    location="MyKeyStoreFile.jks"
    type="JKS" password="myPassword"
    pollingRate="5s"
    updateTrigger="polled" />

<!-- A keystore object called defaultKeyStore provides a location, -->
<!-- type, and password. The MyKeyStoreFile.jks file is assumed -->
<!-- to be located in ${server.config.dir}/resources/security -->
<!-- This keystore is configured to be reloaded when the server -->
<!-- recieves an mbean notification to do so -->
  <keyStore id="defaultKeyStore"
    location="MyKeyStoreFile.jks"
    type="JKS" password="myPassword"
    updateTrigger="mbean" />
```

## Full SSL Configuration Example

Here is an example of a full SSL configuration in the `server.xml` file. This example has the following SSL configurations:

- `defaultSSLSettings`
- `mySSLSettings`

By default, the SSL configuration is set to `defaultSSLConfig`.

```
<featureManager>
  <feature>ssl-1.0</feature>
</featureManager>

<!-- default SSL configuration is defaultSSLSettings -->
<sslDefault sslRef="defaultSSLSettings" />
<ssl id="defaultSSLSettings"
  keyStoreRef="defaultKeyStore"
  trustStoreRef="defaultTrustStore"
  clientAuthenticationSupported="true" />
<keyStore id="defaultKeyStore"
  location="key.jks"
  type="JKS" password="defaultPWD" />
<keyStore id="defaultTrustStore"
  location="trust.jks"
  type="JKS" password="defaultPWD" />

<ssl id="mySSLSettings"
  keyStoreRef="myKeyStore"
  trustStoreRef="myTrustStore"
  clientAuthentication="true" />
<keyStore id="LDAPKeyStore"
  location="{server.config.dir}/myKey.p12"
  type="PKCS12"
  password="{xor}CDo9Hgw=" />
<keyStore id="LDAPTrustStore"
  location="{server.config.dir}/myTrust.p12"
  type="PKCS12"
  password="{xor}CDo9Hgw=" />
```

## Liberty:Keystores

Liberty can create only a keystore type of Java Keystore (JKS). Support for other types of keystore in Liberty can depend on what is supported by the underlying Java Runtime Environment (JRE). The following are the different keystore types in Liberty.

For more information on configuration attributes of the keystore element, see “Liberty:SSL configuration attributes” on page 1835.

## JKS and JCEKS

Java Keystore (JKS) and Java Cryptography Extensions Keystore (JCEKS) are common between the IBM JRE and the Oracle JRE, and can be configured the same using either JRE. JKS is the default keystore type in Liberty, and the only type of keystore Liberty can create. If no keystore type is specified in the configuration, JKS is used.

An example of JKS keystore configuration is as follows:

```
<keyStore id="sampleJKSKeyStore"
  location="MyKeyStoreFile.jks"
  type="JKS" password="myPassword" />
```

An example of JCEKS keystore configuration is as follows:

```
<keyStore id="sampleJCEKSKeyStore"
  location="MyKeyStoreFile.jceks"
  type="JCEKS" password="myPassword" />
```

8.5.5.9

## PKCS11 keystore

A hardware cryptographic keystore can be configured so that the Liberty server can be used to provide cryptographic token support.

The user must provide a hardware device-specific configuration file. The configuration file is a text file that contains entries in the format of `attribute = value`. The file must contain at least the name and library attribute. For example:

```
name = HWDevice
library = /opt/foo/lib/libpkcs11.so
```

The name attribute is a name that is being given to this instance of the device. The library attribute contains a path to the library provided by the hardware device to access the device. The configuration file can also contain configuration data specific to the hardware device.

To configure a PKCS11 keystore in Liberty the keystore element must contain the following fields:

- `id` - Uniquely identify the keystore element in the configuration.
- `location` - The path to the hardware device-specific configuration file.
- `type` - PKCS11 must be specified as the keystore type.
- `fileBased` - Must be false to identify this keystore as a device.
- `password` - Password that is needed to access keys in the device.
- `provider` - The provider that is needed. For the IBM JRE, the value must be `IBMPKCS11Impl` and for Oracle JRE it must be `SunPKCS11`.

Here is an example configuration:

```
<keyStore id="hwKeyStore"
  location="${server.config.dir}/HWCrypto.cfg"
  type="PKCS11"
  fileBased="false"
  password="{xor}Lz4sLCgwLTs="
  provider="IBMPKCS11Impl"/>
```

## PKCS12 keystore

Public Key Cryptography Standards #12 (PKCS12) keystore can be used, but not created by Liberty, when you use the IBM JRE. An example of PKCS12 keystore configuration is as follows:

```
<keyStore id="samplePKCS12KeyStore"
  location="MyKeyStoreFile.p12"
  type="PKCS12" password="myPassword" />
```

## CMS keystore

CMS keystore can be configured, but not created by Liberty, when you use the IBM JRE. However, some special configuration is required. The CMS provider is not available by default on the IBM JRE, therefore it must be added to the provider list in the `java.security` file of the IBM JRE. In the following example, the `com.ibm.security.cmskeystore.CMSProvider` class is added to the end of the list. Ensure that the provider number is correct in the provider list. Liberty does not use the CMS keystore stash file to gain access to the keystore.

```

security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.security.jgss.IBMJGSSProvider
security.provider.4=com.ibm.security.cert.IBMCertPath
security.provider.5=com.ibm.security.sasl.IBMSASL
security.provider.6=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.7=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.8=org.apache.harmony.security.provider.PolicyProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNego
security.provider.10=com.ibm.security.cmskeystore.CMSProvider

```

To use the CMS keystore, the configuration in the `server.xml` file is as follows:

```

<keyStore id="sampleCMSKeyStore"
password="myPassword"
location="MyKeyStoreFile.kdb"
provider="IBMCMSProvider"
type="CMSKS"/>

```

z/OS

## RACF keyring types

RACF keyrings can be used, but not created by Liberty, as keystores on z/OS. The two keyring types that are available are JCERACFKS and JCEHYBRIDRACFKS.

### JCERACFKS keystore

JCERACFKS is a RACF keyring type. You must set up RACF before Liberty can use it. Supply a URL to the keyring in the `location` attribute, and set the `fileBased` attribute to `false`.

An example of using the JCERACFKS keystore is as follows:

```

<keyStore id="sampleKeyring" location="safkeyring:///Keyring"
type="JCERACFKS" password="password" fileBased="false"
readOnly="true" />

```

### JCEHYBRIDRACFKS keystore

JCEHYBRIDRACFKS is a special keyring that checks whether a hardware keystore type is configured. If the JCEHYBRIDRACFKS keystore is not configured, the RACF keyring is used. It is supported on IBM Java 7 SR3 and later. You must edit the `java.security` file and add the `com.ibm.crypto.ibmjcehybrid.provider.IBMJCEHYBRID` class to the top of the provider list. Ensure that the provider numbers are adjusted for the new entry.

An example of using the JCEHYBRIDRACFKS keystore is as follows:

```

<keyStore id="sampleHybridKeyring" location="safkeyringhybrid:///HybridKeyring"
type="JCEHYBRIDRACFKS" password="{xor}Lz4sLCgwLTs=" fileBased="false"
readOnly="true" />

```

## Enabling the IBM JCE Hybrid Provider for Liberty

The IBM JCE Hybrid Provider `IBMJCEHYBRID`, is for use by an application that is designed to use cryptographic hardware and processors when they are available, but continues without those cryptographic features when they are not available. Using the `IBMJCEHYBRID` provider enables an application to take advantage of JCE providers without having to include complex error handling for when cryptographic features are not available.

### Before you begin

Ensure that the `IBMJDK` running on z/OS is at Java 7 SR3 or later.

## | About this task

| The IBMJCEHYBRID provider does not do any cryptographic operations, but routes requests to JCE providers registered with the Java Security Framework. The IBMJCEHYBRID provider must be the first JCE provider in the active JVM provider list, which is initialized from the `java.security` provider list. The IBMJCEHYBRID provider routes requests to, and provides failover for, JCE providers according to the security provider registrations done at JVM initialization. This function enables an application to take advantage of cryptographic features when they are available and to use a provider that does not depend on these features when they are not available.

## | Procedure

1. Add the provider to the `java.security` file with the hardware cryptographic provider.

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.ibmjcehybrid.provider.IBMJCEHYBRID
security.provider.3=com.ibm.crypto.hwcca.provider.IBMJCECCA
security.provider.4=com.ibm.crypto.provider.IBMJCE
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.security.sasl.IBMSASL
```
2. Configure the keyring in `file server.xml` to set the location to use `safkeyringhybrid`, and the type to `JCEHYBRIDRACFKS`. The following example shows the definition of a minimal SSL configuration keystore.

```
<keyStore id="defaultKeyStore" location="safkeyringhybrid:///mykeyring" type="JCEHYBRIDRACFKS"
password="{<u>xor</u>Lz4sLCgwTs=" fileBased="false" readOnly="true"/>
```

## | SSL defaults in Liberty

8.5.5.7

Specifies the default SSL certificate, keystore, and configuration in Liberty.

### Default Certificate and keystore

As a convenience tool to help developers get up and running, users can use the **createSSLCertificate** parameter in the **securityUtility** command to create self-signed certificates. Users can either call the tool directly from the command line or let the server call it to create the default certificate and keystore on server startup.

The server creates the default keystore and certificate if a user has a keystore element that is called `defaultKeyStore` in the `server.xml` file. For example:

```
<keyStore id="defaultKeyStore" password="yourPassword" />
```

If a keystore configuration for the `defaultKeyStore` is in place and the keystore does not exist when the server starts, the server calls the **createSSLCertificate** parameter to create the keystore with a password that is specified in the configuration.

Default keystore details:

- Location: The keystore file is called `key.jks` and is in the `server` or `clients` `resources/security` directory.
- Keystore type: The keystore type is `JKS`.
- Password: Password that is provided in the configuration.

Default certificate that is created by Liberty details:

- Type: The certificate is a self-signed certificate.
- Size: The default certificate size is 2048.
- Signature algorithm: The signature algorithm for the certificate is `SHA256WITHRSA`.

- Validity: The certificate is valid for 365 days.
- SubjectDN: The certificate gets created with CN=<hostname>,OU=<client or server name>,O=ibm,C=US as the SubjectDN.

The **createSSLCertificate** parameter can be called on the command line if users would like to customize the certificate.

**Note:** When the use of a collective controller is not practical, perhaps there is only one or two Liberty servers, a self-signed certificate can be used to restrict the number of clients that can connect to the Liberty member server. It is suggested that an IHS server is used in front of the Liberty servers, where an appropriate CA signed certificate can be used, along with CN whitelisting to control which clients can connect to HIS. A trusted channel between IHS and the Liberty Member server can be maintained by using the self signed certificate.

## Default SSL configuration

The minimal configuration that is needed for SSL is a single keystore element called `defaultKeyStore`. When the `defaultKeyStore` exists in the configuration the run time builds an SSL configuration that is called `defaultSSLConfig` around it.

`defaultSSLConfig` details:

- Protocol: When the IBM JRE is used, the protocol is set to `SSL_TLS` by default. If the Oracle JRE is used SSL is used as the protocol.
- Ciphers: The cipher list is built by getting a list of supported ciphers from the underlying JRE. By default the list is reduced to all the ciphers that are 128 bit and higher or 3DES. RC4 is removed because they are not considered safe to have enabled. ECDHE ciphers are removed because they can cause errors if you are going to a server that does not support them. The cipher list can be customized to include them.
- Client authentication: By default `clientAuthentication` and `clientAuthenticationSupported` are disabled.
- Keystore: In the default configuration `defaultKeyStore` is used as both the key and truststore.

An `ssl` element that is called `defaultSSLConfig` can be entered in the `server.xml` file for customization of the SSL configuration properties. A customized `ssl` element that is called `defaultSSLConfig` is still treated like the default SSL configuration as long as a different SSL configuration has not been identified as the default. For more information on attributes that can be used to customize an SSL configuration, see `SSL configuration attributes`.

To designate a different `ssl` element in the configuration as the default SSL configuration, users can identify that with the `sslDefault` element.

```
<sslDefault sslRef="customSSLConfiguration" />
```

The attributes from the Liberty default SSL configuration are used to create an `SSLContext`. That `SSLContext` is set on the process as the default `SSLContext` by using the Java API `SSLContext.setDefault()`. If an application makes a call to an API like `URLConnection()` with an `https` URL and does not provide any SSL information, then the application picks up the default `SSLContext` of the process and in this case is the `SSLContext` that is created with the Liberty default SSL configuration.

If there is no default SSL configuration in Liberty, then the JSSE's default `SSLContext` is used. The JSSE's default `SSLContext` uses the `cacerts` file for the keystore and truststore. There is no default SSL configuration in Liberty if there is no SSL feature that is defined or if the SSL configuration that exists is not identified as the default. The default configuration is either the called `defaultSSLConfig`, which can be implicit if a `defaultKeyStore` is defined or an alternative SSL configuration can be designated by using the `sslDefault` element.

The `javax` system properties, `javax.net.ssl.keystore`, is used to set up the keystore and truststore information for the default SSL context and must not be used. If the properties are set on the process, then the call to `SSLContext.setDefault()` wipes them out.

## Creating SSL certificates for your Liberty using the Utilities menu

Using the Liberty Utilities menu in the developer tools, you can create an SSL certificate.

### Procedure

1. In the Servers view, right-click your Liberty server, and select **Utilities > Create SSL Certificate**.
2. On the Create SSL Certificate page, you can create a default secure socket layer (SSL) certificate to use with your server.
  - a. In the **Keystore password** field, type a password for your SSL certificate.
  - b. Click the **Specify validity period (days)** field, and specify the number of days you want the certificate to be valid for. Minimum length of time is 365 days.
  - c. Click the **Specify subject (DN):** field, and provide a value for your SSL subject.
3. Click **Finish**.

## Creating SSL certificates from the command line

You can use the `securityUtility` command to create a default SSL certificate for use by the Liberty configuration.

### Procedure

1. Open a command line, then change directory to the `wlp/bin` directory.
2. Create an SSL certificate.

Run the following command. If you do not specify a server name or a password, the command does not run. See “Liberty:securityUtility command.”

```
securityUtility createSSLCertificate --server=server_name --password=your_password
```

### Results

You have created a default keystore `key.jks` for the specified server. The keystore file is located under the `/resources/security` directory of the specified server. If a default keystore already exists, the command does not execute successfully.

### What to do next

You can configure your server to use the keystore and enable the SSL in the server configuration by adding the following lines to the server configuration file:

```
<featureManager>  
  <feature>ssl-1.0</feature>  
</featureManager>  
  
<keyStore id="defaultKeyStore" password="keystore_password" />
```

See “Enabling SSL communication in Liberty” on page 1834.

### Liberty:securityUtility command

The `securityUtility` command supports plain text encryption and SSL certificate creation for Liberty.

### Syntax

The command syntax is as follows:

```
securityUtility task [options]
```

Where the **options** are different based on the value of **task**.

## Parameters

The following tasks are available for the `securityUtility` command:

### encode

Encodes the provided *text* by using Base64. If no options are specified, the command enters interactive mode. Otherwise, the provided *text* is encoded. If the *text* includes spaces it must be put in quotation marks.

#### 8.5.5.0

The options are:

#### **--encoding=encoding\_type**

Specifies how to encode the password. Supported encodings are `xor`, `aes`, and `hash`. If this option is not provided, the default is `xor`.

**Note:** The hash encoding option is used for encoding passwords for the basic user registry only.

#### **--key=encryption\_key**

Specifies the key to be used when encoding using AES encryption. This string is hashed to produce an encryption key that is used to encrypt and decrypt the password. The key can be provided to the server by defining the variable `wlp.password.encryption.key` whose value is the key. If this option is not provided, a default key is used.

#### **--notrim**

Specify whether space characters are removed from the beginning and end of the specified text. If this option is specified, the provided text is encoded as it is. If this option is not specified, space characters from the beginning and end of the specified text is removed.

*text* The text that is to be encoded.

See also “Liberty: The limits to protection through password encryption” on page 1009.

### createSSLCertificate

Creates a default keystore including an SSL certificate for use in a server or client configuration.

#### 8.5.5.6

#### **Keystore details:**

location: In the server's or client's directory under `resource/security/key.jks`.

type: JKS

password: Password provided with the `--password` option. The password is needed to open the keystore file and retrieve the key from the keystore file.

#### 8.5.5.6

#### **Certificate details:**

type: Self-signed certificate

size: 2048 by default, alternate size can be specified with the `--keySize` option.

signature algorithm: SHA256withRSA, can be customized with the `--sigAlg` option.

validity: 365 days by default, can be customized with the `--validity` option.

SubjectDN: CN=<hostname>,OU=<client or server name>,O=ibm,C=us by default, can be customized with the `--subject` option.

The options are:

**8.5.5.6 --server=name**

Specifies the name of the Liberty server for which the keystore and certificate is created. This option cannot be used if the `--client` option is specified.

**8.5.5.6 --client=name**

Specifies the name of the Liberty client for which the keystore and certificate is created. This option cannot be used if the `--server` option is specified.

**8.5.5.6 --keySize=size**

Specifies the certificate key bit size. The default value is 2048.

**--password=password**

Specifies the password to be used in the keystore, which must be at least 6 characters in length. This option is required.

**--passwordEncoding=password\_encoding\_type**

Specifies how to encode the keystore password. Supported encoding value is `xor` or `aes`. If this option is not provided, a default value of `xor` is used.

**--passwordkey=password\_encryption\_key**

Specifies the key to use to encode the keystore password by using AES encryption. This string is hashed to produce an encryption key that is used to encrypt and decrypt the password. The key can be provided to the server by defining the variable `wlp.password.encryption.key` whose value is the key. If this option is not provided, a default key is used.

**--validity=days**

Specifies the number of days that the certificate is valid, which must be equal to or greater than 365. If this option is not provided, a default value of 365 is used.

**8.5.5.6 --subject=DN**

Specifies the Distinguished Name (DN) for the certificate subject and issuer. If this option is not provided, a default value of `CN=<hostname>,OU=<server or client name>,O=ibm,C=us` is used. The CN value is retrieved by using a java method to get the machine's local host name. If the host name cannot be resolved, the IP address is returned.

**8.5.5.7 --sigAlg**

Specifies the signature algorithm that is used to sign the self-signed certificate. The signature algorithm that is supported depends on what is supported by the underlying JRE. Stronger signature algorithms might require the JRE to have the unrestricted policy file in place.

The command accepts `SHA256withRSA` (default), `SHA1withRSA`, `SHA384withRSA`, `SHA512withRSA`, `SHA1withECDSA`, `SHA256withECDSA`, `SHA384withECDSA`, and `SHA512withECDSA`. The signature algorithms that end with `RSA` creates certificates with `RSA` keys and those that end with `ECDSA` creates certificates with `Elliptical Curve (EC)` keys.

**Note:** If you are using certificates that are created with `EC` keys, then your server needs a customized ciphers list in the `ssl` configuration to include `EC` ciphers.

**help** Prints help information for a specified task.

## Usage

The following examples demonstrate correct syntax:

```
securityUtility encode
```

### 8.5.5.0

```
--encoding=aes GiveMeLiberty securityUtility createSSLCertificate --server=myserver  
--password=myspassword --validity=365 --subject=CN=mycompany,O=myOrg,C=myCountry  
securityUtility help createSSLCertificate
```

#### CAUTION:

Different operating system might treat some characters differently. For the Windows environment, if you have ! in your input string, it needs to be escaped by the ^ character. For example,

```
D:\Liberty\images\855\Liberty855\wlp\bin>securityUtility encode "a^!"
```

## Configuring your web application and server for client certificate authentication

You can configure your web application on Liberty using SSL client authentication.

### Before you begin

This topic assumes that you have already created the SSL certificates, for example as described in “Creating SSL certificates from the command line” on page 1844.

### About this task

Client certificate authentication occurs if the server-side requests that the client-side send a certificate. A WebSphere server can be configured for client certificate authentication on the SSL configuration. To do this, you add the `ssl-1.0` Liberty feature to the `server.xml` file, along with code that tells the server the keystore information for authentication.

For details of which aspects of SSL are supported, see “Liberty features” on page 826.

### Procedure

1. Ensure that the deployment descriptor for your web application specifies client certificate authentication as the authentication method to use.

Check that the deployment descriptor includes the following element:

```
<auth-method>CLIENT-CERT</auth-method>
```

**Note:** You can use a tool such as Rational Application Developer to create the deployment descriptor.

2. Optional: Generate an SSL certificate using the command line. See “Liberty:securityUtility command” on page 1844.
3. Configure your server to enable SSL client authentication by adding the following lines to the `server.xml` file:

```
<featureManager>  
  <feature>ssl-1.0</feature>  
</featureManager>  
  
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore"  
  trustStoreRef="defaultTrustStore" clientAuthenticationSupported="true" />  
<keyStore id="defaultKeyStore" location="key.jks" type="JKS" password="defaultPWD" />  
<keyStore id="defaultTrustStore" location="trust.jks" type="JKS" password="defaultPWD" />
```

- If you specify `clientAuthentication="true"`, the server requests that a client sends a certificate. However, if the client does not have a certificate, or the certificate is not trusted by the server, the handshake does not succeed.
- If you specify `clientAuthenticationSupported="true"`, the server requests that a client sends a certificate. However, if the client does not have a certificate, or the certificate is not trusted by the server, the handshake might still succeed.

- If you do not specify either `clientAuthentication` or `clientAuthenticationSupported`, or you specify `clientAuthentication="false"` or `clientAuthenticationSupported="false"`, the server does not request that a client send a certificate during the handshake.
4. Add a client certificate to your browser. See the documentation of your browser for adding client certificates.
  5. Make sure the server trusts any client certificates that are used.
  6. Make sure any client certificates used for client authentication are mapped to a user identity in your registry.
    - For the basic registry, the user identity is the common name (CN) from the distinguished name (DN) of the certificate.
    - For a Lightweight Directory Access Protocol (LDAP) registry, the DN from the client certificate must be in the LDAP registry.
  7. To use basic authentication, user ID and password only, if client certificate authentication does not succeed, add the following line to your `server.xml` file.
 

```
<webAppSecurity allowFailOverToBasicAuth="true" />
```

**Note:** If you specify `allowFailOverToBasicAuth="false"` or do not specify `allowFailOverToBasicAuth`, and the client certificate authentication does not succeed, the request generates a 403 Authentication error message, and the client is not prompted for basic authentication.

## Setting up Liberty to run in SP800-131a

8.5.5.0

You can set up Liberty to meet the SP800-131a requirement that is originated by the National Institute of Standards and Technology (NIST).

### About this task

SP800-131a requires longer key lengths and stronger cryptography. The specification also provides a configuration that enables users to move to a strict enforcement of SP800-131a. The configuration also enables users to run with a mixture of settings from both FIPS140-2 and SP800-131a. SP800-131a can be run in two modes, transition and strict. The transition mode is offered to give user a setting to move their environment to SP800-131a strict mode. In transition mode, it is optional to use the SP800-131a required certificates and to set the protocol to SP800-131a

Strict enforcement of SP800-131a requirements on Liberty includes the following:

- The use of the TLSv1.2 protocol for the Secure Sockets Layer (SSL) context.
- Certificates must have a minimum length of 2048. Elliptical Curve (EC) certificate require a minimum size of 244-bit curves.
- Certificates must be signed with a signature algorithm of SHA256, SHA384, or SHA512. Valid signatureAlgorithms include:
  - SHA256withRSA
  - SHA384withRSA
  - SHA512withRSA
  - SHA256withECDSA
  - SHA384withECDSA
  - SHA512withECDSA

**Note:** If SHA384withECDSA or SHA512withECDSA is used, the unrestricted policy file needs to be in place for the IBM JDK.

- SP800-131a approved Cipher suites.

**Note:** To configure a Liberty server to run in SP800-131a mode, users must be running with a level of the IBM JDK that supports SP800-131a. The minimal levels of the IBM JDK include Java 6 sr 10, Java 6.0.1 sr 2, or Java 7.

For more information about the SP800-131a standard, see the National Institute of Standards and Technology.

You can configure Liberty to run in SP800-131a strict mode or transition mode as following:

## Procedure

- Configure Liberty to run in SP800-131a strict mode.
  1. Make sure that you are running on a level of the IBM JDK that supports SP800-131a.
  2. Make sure that certificates of your server meet the criteria for SP800-131a.
    - Certificates have a minimum length of 2048 and Elliptical Curve (EC) certificates have a minimum size of 244-bit curve.
    - Certificates are signed with at least SHA256 or signed with one of the signature algorithms listed previously.
  3. Configure your SSL Configuration to use the TLSv1.2 protocol. See “Enabling SSL communication in Liberty” on page 1834 and “Liberty:SSL configuration attributes” on page 1835 for more details.
  4. When using collectives, if the `sslProtocol` is updated, two configuration changes must be made:
    - `${wlp.install.dir}/etc/server.env` must specify the `-Dhttps.protocols` property in order for the `${wlp.install.dir}/bin/collective` utility to successfully communicate with the controller.  
For example:

```
JVM_ARGS=-Dhttps.protocols=TLSv1.2
```
    - Each internal collective replication `ssl id` must be updated with the desired protocol.  
For Example:

```
<ssl id="controllerConnectionConfig" sslProtocol="TLSv1.2"/>
<ssl id="memberConnectionConfig" sslProtocol="TLSv1.2"/>
```
  5. Optional: If Elliptical Curve (EC) ciphers are required, list them in the **enabledCiphers** attribute. EC ciphers are not included when cipher lists are generated using the **securityLevel** attribute of the SSL Configuration. For the full list of ciphers, see the Java Technology Security information.
  6. The Java Secure Socket Extension (JSSE) is enabled to run in SP800-131a strict mode by setting the system property `com.ibm.jsse2.sp800-131` to *strict*. For example, `-Dcom.ibm.jsse2.sp800-131=strict`. See “Customizing the Liberty environment” on page 1565 for how to set system properties in the `jvm.options` file.
- Configure Liberty to run in SP800-131a transition mode.
  1. Make sure that you are running a level of the IBM JDK that support SP800-131a.
  2. Optional: If Elliptical Curve (EC) ciphers are required, list them in the **enabledCiphers** attribute. EC ciphers are not included when cipher lists are generated using the **securityLevel** attribute of the SSL Configuration. For the full list of ciphers, see the Java Technology Security information.
  3. The JSSE is enabled to run in SP800-131a transition mode by setting the system property `com.ibm.jsse2.sp800-131` to *transition*. For example, `-Dcom.ibm.jsse2.sp800-131=transition`. See “Customizing the Liberty environment” on page 1565 for how to set system properties in the `jvm.options` file.

**Note:** If you change your protocol to use TLSv1.2, make sure that your browser supports TLSv1.2.

## Configuring an httpEndpoint to use an SSL configuration other than the default

By default, an httpEndpoint element uses the server default SSL configuration, defaultSSLConfig. You can configure an httpEndpoint to use an SSL configuration other than the default SSL configuration.

### About this task

You can configure an httpEndpoint to use an SSL configuration in multiple ways. The following examples show different ways to configure an httpEndpoint to use an SSL configuration other than the default SSL configuration.

### Procedure

- Set the SSL options directly on the httpEndpoint. The following example shows how to set the SSL options on the httpEndpoint, and assumes that you have an SSL configuration that is named wasListenerSSLConfig already defined that is not in this example:

```
<httpEndpoint id="defaultHttpEndpoint"
  host="${listener.host}"
  httpPort="${http.port}"
  httpsPort="${https.port}">
  <sslOptions sslRef="wasListenerSSLConfig" />
</httpEndpoint>
```

- Reference an sslOption element in the httpEndpoint. The following example shows how to reference an sslOption element, and assumes that you have an SSL configuration that is named wasListenerSSLConfig already defined that is not in this example:

```
<sslOptions id="mySSLOptions" sslRef="wasListenerSSLConfig" />
```

```
<httpEndpoint id="defaultHttpEndpoint"
  host="${listener.host}"
  httpPort="${http.port}"
  httpsPort="${https.port}"
  sslOptionsRef="mySSLOptions"
/>
```

- Change the default sslOptions element to point to an SSL configuration other than the default SSL configuration. This option does not alter the httpEndpoint. The following example shows how to change the default sslOptions element, and assumes that you have an SSL configuration that is named wasListenerSSLConfig already defined that is not in this example:

```
<sslOptions id="defaultSSLOptions" sslRef="wasListenerSSLConfig" />
```

---

## Authenticating users in Liberty

The Liberty server uses a user registry to authenticate a user and retrieve information about users and groups to perform security-related operations, including authentication and authorization.

### About this task

To learn about how authentication works in Liberty, see “Liberty:Authentication” on page 976.

The authentication tasks that you can configure might vary depending on your requirements. Unless you have used the quickStartSecurity element that can configure only one user, you have to configure the user registry at the least. You do not have to configure the values for JAAS, authentication Cache and SSO tasks unless you want to change the default values. Configure TAI configuration only when you have an implementation of TAI interface to handle authentication.

You can complete one or more of the following authentication tasks:

## Procedure

- Configure authentication cache in Liberty
- Configure a custom JAAS login module for Liberty
- Configure SSO on Liberty
- Configure a user registry for Liberty
- Configure RunAS authentication in Liberty
- Configure TAI for Liberty

## Configuring a user registry for Liberty

You can store user and group information for authentication in several types of registries. For example you can use a basic user registry, an LDAP registry, or a Custom User Registry. **8.5.5.0** Optionally, you can configure two or more LDAP registries so that the operations are executed on all the configured registries. For example, when you perform an operation of searching a user, the search is performed on all the configured LDAP registries. **z/OS** For z/OS systems, you can use a SAF registry.

## Procedure

- Configure a basic user registry for Liberty
- Configure an LDAP user registry for Liberty
- **z/OS** Configure the SAF registry for Liberty on z/OS(r)

## Configuring a basic user registry for Liberty

You can configure a basic user registry in Liberty for authentication.

## About this task

You can use a basic user registry by defining the users and groups information for authentication on the Liberty server. To do this, you add the appSecurity-2.0 Liberty feature to the server.xml file, along with user information in the basicRegistry element.

## Procedure

1. Add the appSecurity-2.0 Liberty feature to the server.xml file.
2. Optional: To use SSL, add the ssl-1.0 Liberty feature in the server.xml file. See “Enabling SSL communication in Liberty” on page 1834.
3. Configure the basic registry for the server as follows:

```
<basicRegistry id="basic" realm="customRealm">
  <user name="mlee" password="p@ssw0rd" />
  <user name="rkumar" password="pa$$w0rd" />
  <user name="gjones" password="{xor}Lz4sLCgwLTs=" />
  <group name="students">
    <member name="mlee" />
    <member name="rkumar" />
  </group>
</basicRegistry>
```

### Notes:

- You must use unique names for your users and groups.
- You should remove all trailing and leading spaces from the user and group names.
- If user ID or password contains characters other than US-ASCII, make sure that the file is saved by using UTF-8 character encoding.
- **Distributed operating systems** If you use the WebSphere Application Server Developer Tools for Eclipse, the password is encoded for you automatically.

- If you edit the `server.xml` file directly, you can use the **securityUtility encode** command to encode the password for each user. The `securityUtility` command-line tool is available in the `$INSTALL_ROOT/bin` directory. When you run the **securityUtility encode** command, you either supply the password to encode as an input from the command line or, if no arguments are specified, the tool prompts you for the password. The tool then outputs the encoded value. Copy the value output by the tool, and use that value for the password. For example, to encode the password `GiveMeLiberty`, run the following command:  
**securityUtility encode GiveMeLiberty**
- **8.5.5.0** There are several security configuration examples on the `WASdev.net` website for reference when configuring security for your applications on Liberty.

## Configuring LDAP user registries in Liberty

You can configure one or more Lightweight Directory Access Protocol (LDAP) servers in Liberty for authentication.

### Before you begin

Ensure that your LDAP server is up and running, and that the host name and port number of the LDAP server are already in your known list.

### About this task

You can use an existing LDAP server for application authentication in Liberty. **8.5.5.0** To do this, you add the `appSecurity-2.0` feature to the `server.xml` file and specify, in the `server.xml` file, the `ldapRegistry-3.0` feature, and the configuration information for connecting to the LDAP server.

**Avoid trouble:** **8.5.5.0** There are several security configuration examples on the `WASdev.net` website for reference when configuring security for your applications on Liberty. For more information, see the link in the related reference for config snippets.

### Procedure

1. **8.5.5.0** Add the `appSecurity-2.0` and `ldapRegistry-3.0` Liberty features to the `server.xml` file.
2. Optional: To communicate with an SSL-enabled LDAP server, add the `ssl-1.0` Liberty feature in the `server.xml` file.
3. Optional: Copy the truststore to the server configuration directory. For example, you can use the `${server.config.dir}` variable.

For SSL communication with an LDAP server to succeed, the Signer certificate for the LDAP server must be added to the truststore that is referenced by the **sslAlias** attribute of the `<ldapRegistry>` element. In the following examples, the Signer certificate must be added to the `LdapSSLTrustStore.jks`.

4. Configure the LDAP entry for the server.

If you do not want SSL for the LDAP server, remove all SSL and keystore-related lines from the following examples.

You configure the LDAP server in the `server.xml` file or by using the WebSphere Application Server Developer Tools for Eclipse. **8.5.5.0** There are several security configuration examples on the `WASdev.net` website for reference when configuring security for your applications on Liberty.

- For IBM Directory Server:

```
<ldapRegistry id="ldap" realm="SampleLdapIDSRealm"
  host="ldapserver.mycity.mycompany.com" port="389" ignoreCase="true"
  baseDN="o=mycompany,c=us"
  ldapType="IBM Tivoli Directory Server"
  sslEnabled="true"
```

```

    sslRef="LDAPSSLSettings">
    <idsFilters
    userFilter="( &uid=%v)(objectclass=ePerson)"
    groupFilter="( &cn=%v)(|(objectclass=groupOfNames)
    (objectclass=groupOfUniqueNames)(objectclass=groupOfURLs)))"
    userIdMap="*:uid"
    groupIdMap="*:cn"
    groupMemberIdMap="mycompany-allGroups:member;mycompany-allGroups:uniqueMember;
    groupOfNames:member;groupOfUniqueNames:uniqueMember">
    </idsFilters>
</ldapRegistry>

<ssl id="LDAPSSLSettings" keyStoreRef="LDAPKeyStore" trustStoreRef="LDAPTrustStore" />

<keyStore id="LDAPKeyStore" location="\${server.config.dir}/LdapSSLKeyStore.jks"
    type="JKS" password="{xor}CDo9Hgw=" />
<keyStore id="LDAPTrustStore" location="\${server.config.dir}/LdapSSLTrustStore.jks"
    type="JKS" password="{xor}CDo9Hgw=" />

```

- For Microsoft Active Directory Server:

```

<ldapRegistry id="ldap" realm="SampleLdapADRealm"
    host="ldapserverserver.mycity.mycompany.com" port="389" ignoreCase="true"
    baseDN="cn=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
    bindDN="cn=testuser,cn=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
    bindPassword="testuserpwd"
    ldapType="Microsoft Active Directory"
    sslEnabled="true"
    sslRef="LDAPSSLSettings">
    <activatedFilters
    userFilter="( &sAMAccountName=%v)(objectcategory=user)"
    groupFilter="( &cn=%v)(objectcategory=group)"
    userIdMap="user:sAMAccountName"
    groupIdMap="*:cn"
    groupMemberIdMap="memberOf:member" >
    </activatedFilters>
</ldapRegistry>

<ssl id="LDAPSSLSettings" keyStoreRef="LDAPKeyStore" trustStoreRef="LDAPTrustStore" />

<keyStore id="LDAPKeyStore" location="\${server.config.dir}/LdapSSLKeyStore.jks"
    type="JKS" password="{xor}CDo9Hgw=" />
<keyStore id="LDAPTrustStore" location="\${server.config.dir}/LdapSSLTrustStore.jks"
    type="JKS" password="{xor}CDo9Hgw=" />

```

If you use the WebSphere Application Server Developer Tools for Eclipse, the `bindPassword` password is encoded for you automatically. If you edit the `server.xml` file directly, you can use the **securityUtility encode** command to encode the `bindPassword` password for you. The `securityUtility` command-line tool is available in the `$INSTALL_ROOT/bin` directory. When you run the **securityUtility encode** command, you either supply the password to encode as an input from the command line or, if no arguments are specified, the tool prompts you for the password. The tool then outputs the encoded value. Copy the value output by the tool, and use that value for the `bindPassword` password.

5. **8.5.0.1** **8.5.5.0** Optional: Configure certificate filter mode for the LDAP server.

```

<ldapRegistry id="LDAP" realm="SampleLdapIDSRealm"
    host="myldap.ibm.com" port="389" ignoreCase="true"
    baseDN="o=ibm,c=us"
    ldapType="IBM Tivoli Directory Server" searchTimeout="8m"
    certificateMapMode="CERTIFICATE_FILTER"
    certificateFilter="uid=${SubjectCN}">
    <idsFilters
    userFilter="( &uid=%v)(objectclass=ePerson)"
    groupFilter="( &cn=%v)(|(objectclass=groupOfNames)
    (objectclass=groupOfUniqueNames)(objectclass=groupOfURLs)))"
    userIdMap="*:uid"
    groupIdMap="*:cn"

```

```

        groupMemberIdMap="ibm-allGroups:member;ibm-allGroups:uniqueMember;
        groupOfNames:member;groupOfUniqueNames:uniqueMember">
    </idsFilters>
</ldapRegistry>

```

For more information about certificate map mode in Liberty, see “Liberty:LDAP certificate map mode” on page 1856.

6. **8.5.5.3** Optional: You can define mapping between LDAP attributes and the user registry <externalId> attribute.

You can define mapping between LDAP attributes and the user registry <externalId> attribute. After the mapping is configured, when you use the user registry <externalId> attribute for any operation, the value will be equivalent to the value of the LDAP attribute that is mapped. The following example code shows the mapping that is defined for the user registry <externalId> attribute with the LDAP <distinguishedName> attribute for the entity type <PersonAccount>. The <autoGenerate> attribute is optional, and the value is false by default.

```

<ldapRegistry id="LDAP" realm="SampleLdapIDSRealm"
  host="myldap.ibm.com" port="389" ignoreCase="true"
  baseDN="o=ibm,c=us"
  ldapType="IBM Tivoli Directory Server" searchTimeout="8m">
  <attributeConfiguration>
    <externalIdAttribute name="distinguishedName" entityType="PersonAccount" autoGenerate="false"></externalIdAttribute>
  </attributeConfiguration>
</ldapRegistry>

```

7. Optional: Configure failover for multiple LDAP servers.

```

<ldapRegistry id="LDAP" realm="SampleLdapIDSRealm"
  host="ldapserver1.mycity.mycompany.com" port="389" ignoreCase="true"
  baseDN="o=ibm,c=us" ldapType="IBM Tivoli Directory Server" idsFilters="ibm_dir_server">
  <failoverServers name="failoverLdapServersGroup1">
    <server host="ldapserver2.mycity.mycompany.com" port="389" />
    <server host="ldapserver3.mycity.mycompany.com" port="389" />
  </failoverServers>
  <failoverServers name="failoverLdapServersGroup2">
    <server host="ldapserver4.mycity.mycompany.com" port="389" />
  </failoverServers>
</ldapRegistry>

```

```

<idsLdapFilterProperties id="ibm_dir_server"
  userFilter="(&uid=%v)(objectclass=ePerson)"
  groupFilter="(&cn=%v)(|(objectclass=groupOfNames)
    (objectclass=groupOfUniqueNames)(objectclass=groupOfURLs))"
  userIdMap="*:uid" groupIdMap="*:cn"
  groupMemberIdMap="ibm-allGroups:member;ibm-allGroups:uniqueMember;
  groupOfNames:member;groupOfUniqueNames:uniqueMember">
</idsLdapFilterProperties>

```

For more information about the ldapRegistry and failoverServers elements, see .

8. **8.5.5.0** Optional: Configure multiple LDAP registries. If multiple LDAP registries are configured in the server.xml file, they are federated automatically. Ensure that the users are unique across all federated repositories, otherwise the user registry operations are not successful.

**Note:** **8.5.5.0** When you use multiple federated LDAP repositories, each repository must define a unique baseDN.

```

<ldapRegistry host="ldapserver1.mycity1.mycompany.com" baseDN="o=mycompany,c=us"
  port="123" ldapType="IBM Tivoli Directory Server">
</ldapRegistry>

<ldapRegistry host="ldapserver2.mycity2.mycompany.com"
  baseDN="cn=users,dc=secfv2,dc=mycity2,dc=mycompany,dc=com"
  port="456"

```

```

    ldapType="Microsoft Active Directory"
    bindDN="cn=testuser,cn=users,dc=secfv2,dc=mycity2,dc=mycompany,dc=com"
    bindPassword="{xor}KzosKyos0i0vKDs=">
</ldapRegistry>

```

**Note:**

- Specifying the federatedRepository element is not mandatory to federate multiple LDAP registries because they are federated automatically. If the federatedRepository element is specified to configure the participatingBaseEntry and primaryRealm elements, then the user registry operations are performed only on the repositories that are defined in the primaryRealm element. You can define the input and output property mappings for different user registry APIs under the primaryRealm element.
- The **name** attribute of the participatingBaseEntry element must be the same as the value of **baseDN** attribute that is specified in the ldapRegistry element. In the example follows, the **baseDN** and **name** attributes are configured for the LDAP registry on the host *ldapsrv1.mycity1.mycompany.com*. The value of **baseDN** attribute must be the same as that of sub tree in your LDAP server and the value of **name** attribute must be the name of that sub tree in the federated user registry. It is optional to specify the **name** attribute. By default, the **name** attribute uses the same value as the **baseDN** attribute. If the **name** attribute is specified in the ldapRegistry element, then the **name** attribute in the participatingBaseEntry element must use the same value as the **name** attribute in the ldapRegistry element.

```

<ldapRegistry host="ldapsrv1.mycity1.mycompany.com" baseDN="o=mycompany,ou=myou,c=us"
    port="123" ldapType="IBM Tivoli Directory Server" name="o=mybaseentry">
</ldapRegistry>

```

```

<ldapRegistry host="ldapsrv2.mycity2.mycompany.com"
    baseDN="cn=users,dc=secfv2,dc=mycity2,dc=mycompany,dc=com"
    port="456"
    ldapType="Microsoft Active Directory"
    bindDN="cn=testuser,cn=users,dc=secfv2,dc=mycity2,dc=mycompany,dc=com"
    bindPassword="{xor}KzosKyos0i0vKDs=">
</ldapRegistry>

```

```

<federatedRepository>
  <primaryRealm name="RealmName" delimiter="@" allowOpIfRepoDown="true">
    <participatingBaseEntry name="o=mybaseentry"/>
    <participatingBaseEntry name="cn=users,dc=secfv2,dc=mycity2,dc=mycompany,dc=com"/>
    <uniqueUserIdMapping inputProperty="uniqueName" outputProperty="uniqueName"/>
    <userSecurityNameMapping inputProperty="principalName" outputProperty="principalName"/>
    <userDisplayNameMapping inputProperty="principalName" outputProperty="principalName"/>
    <uniqueGroupIdMapping inputProperty="uniqueName" outputProperty="uniqueName"/>
    <groupSecurityNameMapping inputProperty="cn" outputProperty="cn"/>
    <groupDisplayNameMapping inputProperty="cn" outputProperty="cn"/>
  </primaryRealm>
</federatedRepository>

```

For more information about the federated ldapRegistry elements, see .

9. **8.5.5.0** Optional: You can configure other optional attributes for the LDAP registry, such as **contextPool** or **ldapCache**, as given in the following example:

```

<ldapRegistry id="IBMDirectoryServerLDAP" realm="SampleLdapIDSRealm"
    host="host.domain.com" port="389" ignoreCase="true"
    baseDN="o=domain,c=us"
    bindDN="cn=testuser,o=domain,c=us"
    bindPassword="mypassword"
    ldapType="IBM Tivoli Directory Server"
    searchTimeout="8m">
  <contextPool enabled="true" initialSize="1" maxSize="0" timeout="0s" waitTime="3000ms" preferredSize="3"/>
</ldapCache>

```

```

    <attributesCache size="4000" timeout="1200s" enabled="true" sizeLimit="2000"/>
    <searchResultsCache size="2000" timeout="600s" enabled="true" resultsSizeLimit="1000"/>
  </ldapCache>
</ldapRegistry>

```

**Note:**

- Federated user registry uses the context pooling mechanism to improve the performance of concurrent access to an LDAP server. Context pooling works at a higher level than the connection pooling. Each context entry in the context pool corresponds to a socket connection to the LDAP server. The bind credentials that are used by this pool are specified when you configure the LDAP registry.
- Federated repository uses the cache mechanism for performance enhancement. It caches information about the LDAP users and groups based on the user operations performed. For example, if you perform a search operation on the LDAP users and groups, the result of the operation is cached. You can enable the `ldapCache` element in the `server.xml` file as shown in the previous example.

**Troubleshooting tip:** **8.5.5.2** To troubleshoot any LDAP authentication issues, use the following trace specifications in the `bootstrap.properties` file:

```
com.ibm.ws.security.wim.*=all:com.ibm.websphere.security.wim.*=all
```

**Liberty:LDAP certificate map mode:** **8.5.0.1**

The certificate map mode is used to specify whether to map X.509 certificates into an LDAP directory by **EXACT\_DN** or **CERTIFICATE\_FILTER** in Liberty.

The **EXACT\_DN** means that the Distinguished Name (DN) in the certificate must exactly match the user entry in the LDAP server, including case and spaces. To use the specified certificate filter for the mapping, you can use the **CERTIFICATE\_FILTER**.

**Certificate filter**

Specifies the filter certificate mapping property for the LDAP filter. The filter is used to map attributes in the client certificate to entries in the LDAP registry.

If more than one LDAP entry matches the filter specification at run time, authentication fails because the result is an ambiguous match. The syntax this filter is:

```
LDAP attribute=${Client certificate attribute}
```

.

An example of a simple certificate filter is: `uid=${SubjectCN}`.

You can also specify multiple properties and values as part of a certificate filter. The LDAP attribute of the filter specification depends on the schema that your LDAP server is configured to use. The client certificate attribute is one of the public attributes in your client certificate. The client certificate attribute must begin with a dollar sign, \$, and opening brace, {, and end with a closing brace, }. The attributes are case-sensitive.

The following LDAP attributes are supported:

- uid
- initials
- sAMAccountName
- displayName
- distinguishedName
- displayName
- description

The following client certificate attributes are supported:

- `${SubjectCN}`
- `${SubjectDN}`
- `${IssuerCN}`
- `${IssuerDN}`
- `${SerialNumber}`

An example of an LDAP configuration with certificate filter mode enabled:

```
<ldapRegistry id="LDAP" realm="SampleLdapIDSRealm"
  host="myldap.ibm.com" port="389" ignoreCase="true"
  baseDN="o=ibm,c=us"
  certificateMapMode="CERTIFICATE_FILTER"
  certificateFilter="uid=${SubjectCN}"
  userFilter="(&(uid=%v)(objectclass=person))"
  groupFilter="(&(cn=%v)(|(objectclass=groupOfNames)
    (objectclass=groupOfUniqueNames)(objectclass=groupOfURLs)))"
  userIdMap="*:uid"
  groupIdMap="*:cn"
  groupMemberIdMap="ibm-allGroups:member;ibm-allGroups:uniqueMember;
    groupOfNames:member;groupOfUniqueNames:uniqueMember"
  ldapType="IBM Tivoli Directory Server" searchTimeout="8m" />
```

## Activating and configuring the SAF registry on z/OS

z/OS

The System Authorization Facility (SAF) registry holds information required to perform security-related functions such as authenticating users and retrieving information about users, groups, or groups associated with users. You activate and configure the SAF registry through the configuration file `server.xml`. In addition, you can configure your Liberty server to use SAF authorization.

### About this task

By adding the appropriate features to the `server.xml` file, you can accomplish the following tasks:

- Activate the SAF user registry
- Configure the SAF user registry to use authorized services
- Enable applications to use the SAF user registry
- Configure the SAF user registry

By default, the SAF registry uses unauthorized UNIX System Services (USS) to perform authentication. For better performance, you can enable the authorized SAF services by configuring the SAFCREDS resources. For more information, see “Enabling z/OS authorized services in Liberty for z/OS” on page 1942.

For information on how to configure your Liberty server to use SAF authorization, see “Configuring authorization for applications in Liberty” on page 1939

### Procedure

1. Activate the SAF user registry. Add the `zosSecurity-1.0` feature to the `server.xml` file:  
`<feature>zosSecurity-1.0</feature>`

**Note:** By default, the SAF user registry uses unauthorized USS services such as `__passwd` to perform authentication.

2. For better performance, configure the SAF user registry to use authorized services such as `initACEE` to perform authentication by configuring the SAFCREDS resources. For more information, see “Enabling z/OS authorized services in Liberty for z/OS” on page 1942.

3. Enable application security by adding the feature `appSecurity-2.0`, along with either the `servlet-3.0` feature for web application, or the `ejbLite-3.1` feature for EJB applications.

```
<feature>zosSecurity-1.0</feature>  
<feature>appSecurity-2.0</feature>  
<feature>servlet-3.0</feature>
```

**8.5.5.0** `<feature>ejbLite-3.1</feature>`

4. Configure the SAF registry by adding a **safRegistry** element in the `server.xml` file:  
`<safRegistry id="saf" realm="myrealm" />`

The **safRegistry** element has the following attributes:

- ID** The ID that uniquely identifies this registry instance. The ID can be anything you want, but must be unique with respect to other configured registries such as the basic registry and the LDAP registry. You can use the ID to refer to this registry instance in other elements of the `server.xml` file.
- realm** The realm associated with the SAF registry. If you do not specify a realm, the default is the plex name (ECVTSPLEX). If the server is authorized to use the SAFCREDS resources, then the default realm is read from the SAF product by extracting the APPLDATA field in the SAFDFLT profile under the REALM class. If that field is empty, then the default realm is used.

#### Mixed-case passwords: **z/OS**

Knowing when a password is interpreted as case sensitive or not can directly affect how you use a local operating system registry. WebSphere Application Server exploits the mixed case password option for the Resource Access Control Facility (RACF), so you can use case sensitive passwords.

Since z/OS Version 1.7, RACF supports the option of a mixed case password. You select this option for RACF by using the **SETROPTS PASSWORD(MIXEDCASE)** command. To use case sensitive passwords in WebSphere Application Server for a local operating system registry, you must comply with all of the following requirements:

- Use z/OS Version 1.7 or later

**Note:** To use Liberty capabilities of z/OS, you must use Version 1.11 or later.

- Use the local operating system registry
- Turn on the RACF mixed case option with the **SETROPTS PASSWORD(MIXEDCASE)** command

**Important:** All three of these requirements must be met; otherwise the WebSphere Application Server password will not be sensitive to case.

If you use a Lightweight Directory Access Protocol (LDAP) configuration, you can use mixed case passwords.

For more information on the mixed case password feature in z/OS Version 1.7, see z/OS V1R7.0 Security Server RACF Security Administrator's Guide. This guide is available under *Security Server and Integrated Security Services*. Within the guide, see section 5.2.1.

There is an SDBM alternative setup for LDAP. For more information, see the topic SDBM authorization in the *Tivoli Directory Server for z/OS* section of the z/OS V1R11 information center.

## Configuring SCIM for user and group member management

**8.5.5.8**

You can configure the scim-1.0 feature in the server.xml file to enable user and group member management. System for Cross-domain Identity Management (SCIM) defines REST APIs to create, retrieve, update, and delete (CRUD) users and groups. Calls are made through a systems management REST WAB. The local calls will be HTTP over localhost through Web API only; no java APIs for local calls.

## Procedure

Adding the scim-1.0 feature in the server.xml file enables SCIM functions. But to complete the configuration, you must also perform the following configuration steps:

- **SSL Configuration:** The REST services are protected and can be accessed only on the HTTPS port. For more information about how to complete the SSL configuration, see “Enabling SSL communication in Liberty” on page 1834.
- **Configuration of Federation Registry:** The SCIM functions is only supported by the Federation Registry. To quickly set up a federation registry by using LDAP, see “Configuring LDAP user registries in Liberty” on page 1852.
- **Configuration of an administrator role:** The REST services are only accessible by an administrator, so a user needs to be configured with an administrator role. For more information about mapping the administrator role to Liberty, see “Mapping the administrator role for Liberty” on page 1644.

**Note:** For configuration of the administrator role for SCIM, you cannot use the Quick Start Registry.

- **Configuration of HTTPS port (optional):** The HTTP end point must be configured. For more information about the httpEndpoint feature element configuration, see the httpEndpoint section in “Admin Center” on page 855.

After the configuration steps are completed, the scim-1.0 feature is now ready to be used. A sample configuration in the server.xml file is shown in the following example:

```
<server description="server1">
  <!-- Enable features -->
  <featureManager>
    <feature>appSecurity-2.0</feature>
    <feature>servlet-3.0</feature>
  <feature>ldapRegistry-3.0</feature>
  <feature>scim-1.0</feature>
  <feature>ssl-1.0</feature>
  </featureManager>

  <httpEndpoint id="defaultHttpEndpoint" httpPort="9080" httpsPort="9090">
    <tcpOptions soReuseAddr="true" />
  </httpEndpoint>

  <ldapRegistry id="LDAP1" realm="SampleLdapIDSRealm" host="9.127.1.90" port="1389" ignoreCase="true"
    baseDN="o=ibm,c=us" ldapType="IBM Tivoli Directory Server" searchTimeout="8m" recursiveSearch="true"
    bindDN="cn=xxxx" bindPassword="xxxxxx">
    <ldapEntityType name="PersonAccount">
      <rdnProperty name="uid" objectClass="inetOrgPerson"/>
      <objectClass>inetOrgPerson</objectClass>
    </ldapEntityType>
    <ldapEntityType name="Group">
      <objectClass>groupofnames</objectClass>
    </ldapEntityType>
  </objectClass>ibm-nestedGroup</objectClass>
  <rdnProperty name="cn" objectClass="groupofnames"/>
  </ldapEntityType>
  <attributeConfiguration>
    <attribute name="title" propertyName="honorificPrefix" syntax="String" entityType="PersonAccount">
      </attribute>
  </attribute name="initials" propertyName="middleName" syntax="String" entityType="PersonAccount">
    </attribute>
  </attribute name="st" propertyName="honorificSuffix" syntax="String" entityType="PersonAccount">
```

```

        </attribute>
<attribute name="l" propertyName="homeStateOrProvinceName" syntax="String" entityType="PersonAccount">
    </attribute>
<attribute name="street" propertyName="homeStreet" syntax="String" entityType="PersonAccount">
    </attribute>
<attribute name="postalAddress" propertyName="homeCity" syntax="String" entityType="PersonAccount">
    </attribute>
<attribute name="postalCode" propertyName="homePostalCode" syntax="String" entityType="PersonAccount">
    </attribute>
    <attribute name="postOfficeBox" propertyName="homeCountryName" syntax="String" entityType="PersonAccount">
    </attribute>
    <attribute name="departmentNumber" propertyName="photoURLThumbnail" syntax="String" entityType="PersonAccount">
    </attribute>
<attribute name="description" propertyName="photoURL" syntax="String" entityType="PersonAccount">
    </attribute>
</attributeConfiguration>
<groupProperties>
    <memberAttribute name="member" dummyMember="uid=dummy" objectClass="groupOfNames" scope="direct"/>
<memberAttribute name="ibm-memberGroup" objectClass="ibm-nestedGroup" scope="direct"/>
</groupProperties>
</ldapRegistry>

<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore" />
<keyStore id="defaultKeyStore" password="Liberty"/>

<administrator-role>
    <user>wasadmin</user>
</administrator-role>

<federatedRepository>
    <primaryRealm name="WIMRegistry">
        <participatingBaseEntry name="o=ibm,c=us"/>
    </primaryRealm>
</federatedRepository>
</server>

```

## SCIM operations in Liberty: 8.5.5.8

The System for Cross-domain Identity Management (SCIM) 1.1 specifications are supported in Liberty.

### Retrieving resources

WebSphere Application Server Liberty supports SCIM 1.1 specifications. For more information about the specification, see <http://www.simplecloud.info/>.

To retrieve a known resource, you must send a GET request to the configured HTTP endpoint. For example, `/Users/{id}` or `/Groups/{id}`.

The following example shows the operations against an LDAP registry.

```

<ldapRegistry id="LDAP1" realm="SampleLdapIDSRealm" host="9.127.1.90" port="1389" ignoreCase="true"
    baseDN="o=ibm,c=us" ldapType="IBM Tivoli Directory Server" searchTimeout="8m" recursiveSearch="true"
    bindDN="xxxxxx" bindPassword="xxxxxx">
    <ldapEntityType name="PersonAccount">
        <rdnProperty name="uid" objectClass="inetOrgPerson"/>
        <objectClass>inetOrgPerson</objectClass>
    </ldapEntityType>
    <ldapEntityType name="Group">
        <objectClass>groupofnames</objectClass>
    </ldapEntityType>
</objectClass>ibm-nestedGroup</objectClass>
    <rdnProperty name="cn" objectClass="groupofnames"/>
</ldapEntityType>

```

```

    <attributeConfiguration>
      <attribute name="title" propertyName="honorificPrefix" syntax="String" entityType="PersonAccount">
        </attribute>
    <attribute name="initials" propertyName="middleName" syntax="String" entityType="PersonAccount">
      </attribute>
    <attribute name="st" propertyName="honorificSuffix" syntax="String" entityType="PersonAccount">
      </attribute>
    <attribute name="l" propertyName="homeStateOrProvinceName" syntax="String" entityType="PersonAccount">
      </attribute>
    <attribute name="street" propertyName="homeStreet" syntax="String" entityType="PersonAccount">
      </attribute>
    <attribute name="postalAddress" propertyName="homeCity" syntax="String" entityType="PersonAccount">
      </attribute>
    <attribute name="postalCode" propertyName="homePostalCode" syntax="String" entityType="PersonAccount">
      </attribute>
    <attribute name="postOfficeBox" propertyName="homeCountryName" syntax="String" entityType="PersonAccount">
      </attribute>
    <attribute name="departmentNumber" propertyName="photoURLThumbnail" syntax="String" entityType="PersonAccount">
      </attribute>
    <attribute name="description" propertyName="photoURL" syntax="String" entityType="PersonAccount">
      </attribute>
    </attributeConfiguration>
  <groupProperties>
    <memberAttribute name="member" dummyMember="uid=dummy" objectClass="groupOfNames" scope="direct"/>
  <memberAttribute name="ibm-memberGroup" objectClass="ibm-nestedGroup" scope="direct"/>
  </groupProperties>
</ldapRegistry>

```

To retrieve a resource from the LDAP, you must send a GET request as `https://localhost:9090/ibm/api/scim/Users/uid=jsmith,o=ibm,c=us`.

## Querying resources

To query resources, you must send a GET request to the configured HTTP endpoint and specify the filter for searching. You can also specify the attributes parameter to return a subset of values from the returned resources and specify the paging and sorting parameters to organize the returned resources. The following examples show some of the filter options:

- Specify the parameter to retrieve subset of the values: For example: `https://localhost:9090/ibm/api/scim/Users?filter=givenname sw` "Jo" retrieves all users whose name starts with "Jo".
- Specify the attributes parameter to retrieve subset of the values: For example: `https://localhost:9090/ibm/api/scim/Users?filter=givenname sw "Jo" &attributes=username,emails&filter=name.familyname eq "Smith"` retrieves the email addresses of the user name that starts with "Jo" and whose family name is "Smith".
- Specify the paging and sorting parameters to retrieve organized resources. For example, `https://localhost:9090/ibm/api/scim/Users?filter=givenname sw "Jo"&attributes=username&sortBy=username&startIndex=3&count=5` retrieves the third page of the sorted result with each page containing five user names that start with "Jo" and whose family name is "Smith".

### Notes:

- The underlying federated repositories determine whether the values that are specified in the filters are case-sensitive. In case of LDAP, the values are not case-sensitive by default, unless the attribute is mapped to a case-sensitive LDAP attribute.
- User name cannot be used in the search filter.
- When federating basic, SAF or custom registries that do not support the SCIM attributes, the filter pattern is always searched against the user name and only the user name attribute is returned.

## Creating resources

To create new resources, you must send a POST request to the resource endpoint, that is, Users or Groups. The POST content must contain the user json object and the HTTP header content-type must be set to application/json.

**Note:** The application/xml content type is not supported.

To create a user, the following request must be posted to `https://localhost:9090/ibm/api/scim/Users`  
Content-Type

Content-Type: application/json

Content-Length: ...

```
{
  "schemas":["urn:scim:schemas:core:1.0"],
  "userName":"bjensen",
  "externalId": "uid=bjensen,o=ibm,c=us",
  "name":{"
    "familyName":"Jensen",
    "givenName":"Barbara"
  }
}
```

The request must contain all the attributes that are required to successfully create a User or Group in the user registry. For example, in a back-end Tivoli Directory Server LDAP, the minimum set of LDAP attributes needed to create a user would be uid, sn, and cn; so any request for creation of user must contain userName, givenName, and familyName. The create operation fails if there are any schema violation from the user registry.

The externalId attribute acts like an identifier and must be specified. The attribute format depends on the specification of back-end user registry. In the previous example, the back-end is an LDAP server with a baseEntry as o=ibm,c=us and the RDN property for the user is set as UID, so the externalId becomes uid=bjensen,o=ibm,c=us.

Based on the create request, the created user object is returned.

```
{
  "schemas":["urn:scim:schemas:core:1.0"],
  "id":"uid=bjensen,o=ibm,c=us",
  "userName":"bjensen",
  "externalId":"uid=bjensen,o=ibm,c=us",
  "name":{"
    "formatted":"Barbara Jensen",
    "familyName":"Jensen",
    "givenName":"Barbara"
  }},
  "meta":{"
    "lastModified":"2015-09-15T14:30:11",
    "location":"https://localhost:9090/ibm/api/scim/Users/uid=bjensen",
    "created":"2015-09-15T14:30:11"
  }
}
```

When more than one LDAPs are configured and a create operation needs to be invoked, a default parent for the entity must be defined. The defined parent specifies the base entry under which the new entity would be created. The following example shows the configuration of a default parent for PersonAccount.

```
<federatedRepository>
  <primaryRealm name="WIMRegistry">
    <participatingBaseEntry name="o=ibm,c=us"/>
    <participatingBaseEntry name="o=ldap"/>
  </primaryRealm>
</supportedEntityType>
```

```

        <defaultParent>o=ldap</defaultParent>
        <name>PersonAccount</name>
    </supportedEntityType>
</federatedRepository>

```

## Modifying resources

To modify resources, one needs to send a PUT request to the resource endpoint, that is, /Users or /Groups. A PUT request performs a complete update of the resource. Any attributes that is not specified in the input are deleted.

**Note:** Partial updates with PATCH are not supported.

To modify the previously created resource, the following request must be posted to `https://localhost:9090/ibm/api/scim/Users/uid=bjensen,o=ibm,c=us`.

```

Content-Type: application/json
Content-Length: ...

```

```

{
  "schemas":["urn:scim:schemas:core:1.0"],
  "userName":"bjensen",
  "externalId":"uid=bjensen,o=ibm,c=us",
  "name":{
    "familyName":"Jensen",
    "givenName":"Barb"
  }
}

```

This request modifies the given name of the object from *Barbara* to *Barb*. The ID specified in the URL must match the `externalId` specified in the user object.

To modify a Group `cn=employeeGroup,o=ibm,c=us` and change the Group membership, the member attribute needs to be specified.

```

Content-Type: application/json
Content-Length: ...

```

```

{
  "id":"cn=employeeGroup,o=ibm,c=us",
  "schemas":["urn:scim:schemas:core:1.0"],
  "displayName":"employeeGroup",
  "externalId":"cn=employeeGroup,o=ibm,c=us",
  "members":[{"value":"uid=bjensen,o=ibm,c=us", "type":"User"}, {"value":"cn=consultants,o=ibm,c=us", "type":"Gr"}
}

```

To modify a Group `cn=employeeGroup,o=ibm,c=us` and remove all the members from a group an empty member attribute needs to be specified.

```

Content-Type: application/json
Content-Length: ...

```

```

{
  "id":"cn=employeeGroup,o=ibm,c=us",
  "schemas":["urn:scim:schemas:core:1.0"],
  "displayName":"employeeGroup",
  "externalId":"cn=employeeGroup,o=ibm,c=us",
  "members":[]
}

```

## Deleting resources

To delete resources, you need to send a DELETE request to the resource endpoint, that is, /Users or /Groups. For example, to delete the user uid=bjensen,o=ibm,c=us that is created in the previous example, send a request to `https://localhost:9090/ibm/api/scim/Users/uid=bjensen,o=ibm,c=us`

**Note:** SCIM runs only on Java 7 or later.

## Configuring additional properties for users and groups

8.5.5.8

You can configure additional properties for users and groups of federated repositories. To enable schema or property extensions, ensure that the property can be read from and written to the underlying repositories.

### Procedure

1. You can specify the following additional property information in the `server.xml` file to enable schema or property extension.
  - Extended Property Name – The name of the extended property. Ensure that the name specified is unique and does not match with an existing property name.
  - Data type – The data type of the extended property. The possible values are Integer, Long, String, Boolean, Date, Double, BigInteger, BigDecimal.
  - Entity type – The entity to which the property applies. The possible values are PersonAccount or Group.

Single or multi-valued - You can set the value of the property to be either single or multi-valued. A default value can also be set for the property. When an entity is created and no value is specified for the property, the default value is used. For a multi-valued property, you can add an extended property named `assetId` for storing assets assigned to a user. If each user can be assigned more than one assets then the `assetId` needs to be multi-valued. You must ensure that the attribute to which the `assetId` is mapped is also a multi-valued attribute in the back-end LDAP .

The following sample shows the configuration in `server.xml`:

```
<federatedRepository>
  <primaryRealm name="WIMRegistry">
    <participatingBaseEntry name="o=ibm,c=us"/>
  </primaryRealm>
  <extendedProperty dataType="String" name="extendedProperty" entityType="PersonAccount"> </extendedProperty>
</federatedRepository>
```

2. To use the extended property in the code, you must use the generic getter/setter methods as shown in the following example:

```
PersonAccount person = new PersonAccount();
...
person.set("extendedProperty", "xyz");
...
String value = (String)person.get("extendedProperty");
```

3. To ensure that property can be read from and written to the LDAP, you have the following two options:
  - Pass-through: If the name of the extended property is same as the name of the LDAP attribute, then the property is passed through and read from and written to the attribute.
  - Property Mapping: If the name of the extended property is different from the name of the LDAP attribute, then the property needs to be mapped by using attribute mapping.

The following sample configuration shows the mapping of the extended property to an attribute named `extendedAttribute`.

```
<attributeConfiguration>
  <attribute name="extendedAttribute" propertyName="extendedProperty" syntax="String" entityType="PersonAccount"><
</attributeConfiguration>
```

## Liberty:Dynamic changes to security

Some specific information on how dynamic configuration changes impact security on Liberty is introduced in this topic.

### Dynamically changing the user registry

Changing the user registry can impact both the server configuration and clients using the server. Before you change the user registry dynamically (without restarting the server), consider the following:

- If you change the user registry type or realm name, all web clients must clear their single sign-on tokens.
- If you change the user registry type or realm name, any values of **accessId** that are specified in the authorization bindings must be updated. The **accessId** takes the form of `user:realmName/uniqueId` or `group:realmName/uniqueId`. The **realmName** in the **accessId** must match the **realmName** for the configuration user registry.

### Developing a custom user repository for Liberty

8.5.5.8

You can develop a custom user repository class by implementing the `com.ibm.ws.security.wim.RepositoryFactory` and `com.ibm.ws.security.wim.Repository` interfaces that are provided in the Liberty server.

#### About this task

The repository interfaces enable support to virtually any type of account repository.

#### Procedure

1. Implement the repository factory (`com.ibm.ws.security.wim.RepositoryFactory`) interface. The `RepositoryFactory` interface gets the configuration parameters and creates an instance of the repository. For example,

```
public Repository getRepository(Map<String, Object> properties) throws WIMException {
    return new CustomRepository(properties);
}
```
2. Implement the repository (`com.ibm.ws.security.wim.Repository`) interface. This class has the actual repository operations.

```
public class CustomRepository extends RepositoryConfiguration implements Repository {

    public CustomRepository(Map<String, Object> properties) {
        System.out.println("Constructor with " + properties);
    }
}
```
3. Convert the implementation class into an OSGi service. For more information, see “Declaring your services to OSGi Declarative Services” on page 1794.
4. Package the custom user repository as an OSGi bundle and export the user repository service. For more information about creating an OSGi bundle, see *Creating an OSGi service bundle*.
5. Create a feature manifest to include the OSGi bundle. For more information, see “Liberty profile: Product extension” on page 967.
6. After the feature is installed into the user product extension location, configure the `server.xml` file with the feature name. For example:

```
<featureManager>
...
<feature>usr:customRepositorySample-1.0</feature>
</featureManager>
```

For a downloadable custom user registry sample, see [https://developer.ibm.com/wasdev/downloads/#asset/samples-Custom\\_User\\_Registry](https://developer.ibm.com/wasdev/downloads/#asset/samples-Custom_User_Registry).

## Example

Refer to the following samples of repository factory and repository interfaces.

### Repository factory interface

```
package com.myorg;

import java.util.Map;

import org.osgi.service.component.ComponentContext;

import com.ibm.websphere.security.wim.exception.WIMException;
import com.ibm.ws.security.wim.Repository;
import com.ibm.ws.security.wim.RepositoryFactory;

public class CustomRepositoryFactory implements RepositoryFactory {

    @Override
    public Repository getRepository(Map<String, Object> properties) throws WIMException {
        System.out.println("getRepository " + properties);
        return new CustomRepository(properties);
    }

    public void activate(ComponentContext cc, Map<String, Object> properties) {
        System.out.println("In activate");
    }

    public void deactivate(ComponentContext cc) {
        System.out.println("In deactivate");
    }
}
```

### Repository interface

```
package com.myorg;

import java.util.Map;

import com.ibm.websphere.security.wim.exception.WIMException;
import com.ibm.websphere.security.wim.model.Root;
import com.ibm.ws.security.wim.Repository;
import com.ibm.ws.security.wim.RepositoryConfiguration;

public class CustomRepository extends RepositoryConfiguration implements Repository {

    public CustomRepository(Map<String, Object> properties) {
        System.out.println("Constructor with " + properties);
    }

    @Override
    public Root create(Root arg0) throws WIMException {
        throw new WIMException("Method not supported");
    }

    @Override
    public Root delete(Root arg0) throws WIMException {
        throw new WIMException("Method not supported");
    }

    @Override
    public Root get(Root arg0) throws WIMException {
        throw new WIMException("Method not supported");
    }
}
```

```

    }

    @Override
    public String getRealm() {
        return "customRepository";
    }

    @Override
    public Root login(Root arg0) throws WIMException {
        throw new WIMException("Method not supported");
    }

    @Override
    public Root search(Root arg0) throws WIMException {
        throw new WIMException("Method not supported");
    }

    @Override
    public Root update(Root arg0) throws WIMException {
        throw new WIMException("Method not supported");
    }
}

```

## Configuring the authentication cache in Liberty

You can modify how authenticated users are cached in Liberty.

### About this task

Because the creation of a subject might impact performance, Liberty provides an authentication cache to store a subject after an authentication of a user is successful. The cache is initialized with a certain number of entries, determined by the **initialSize** attribute, and has a maximum number of entries, determined by the **maxSize** attribute. If the maximum size is reached, then the earliest entries that were used are removed from the cache. If a user has been inactive for longer than period that is specified by the **timeout** attribute, then the entry for that user is removed from the cache. By default, the cache size is initialized to 50 entries and a maximum of 25000 entries, with a timeout of 600 seconds.

You do not have to configure the values for the `authCache` element unless you want to change the default values of the authentication cache.

For more information about authentication case, see “Authentication cache” on page 978.

#### Note:

- Any change that is made to the user registry configuration in the `server.xml` file clears the authentication cache. However, if changes are made to an external user registry, such as LDAP, the authentication cache is unaffected.
- You must consider the following effects of the timeout value on your configuration:
  - Larger authentication cache timeout values can increase security risks. For example, you might revoke a user in the user registry or repository, but the revoked user can log in by using the credential that is cached in the authentication cache until the cache is refreshed.
  - Smaller authentication cache timeout values can affect performance. When this value is smaller, the Liberty server accesses the user registry or repository more frequently.
  - Larger numbers of entries in the authentication cache, which is caused by an increased number of users, increases the memory usage of the authentication cache. Thus, the application server might slow down and affect performance.

## Procedure

1. Enable the appSecurity-2.0 Liberty feature by adding the following code to the server.xml file.

```
<featureManager>
  <feature>appSecurity-2.0</feature>
</featureManager>
```

2. Optional: To change the default options for the authentication cache, add the **<authCache>** element to the server.xml file. In the following example, the initial size of the authentication cache is changed to 100 entries with a maximum of 50000 entries, and the timeout is changed to 15 minutes.

```
<authCache initialSize="100" maxSize="50000" timeout="15m"/>
```

3. Optional: To disable the authentication cache, set the attribute **cacheEnabled** to false in the **<authentication>** element as follows:

```
<authentication id="Basic" cacheEnabled="false" />
```

For more information about the **<authCache>** and **<authentication>** elements, see .

## Configuring a JAAS custom login module for Liberty

You can configure a custom Java Authentication and Authorization Service (JAAS) login module before or after you have configured the Liberty server login module.

### Before you begin

**8.5.5.9** We support the server.xml file, client.xml file and the JAAS configuration file for JAAS configuration. However, it is suggested to configure the JAAS custom login module in the server.xml file or client.xml file. For further details about configuring the JAAS configuration file, see “Configuring an application JAAS custom login context entry and login module using a JAAS configuration file for Liberty” on page 1869.

Make sure you have a JAR file containing the JAAS custom login module, which implements the javax.security.auth.spi.LoginModule interface as described in “Developing JAAS custom login modules for a system login configuration” on page 2002. In this topic, JAAS custom login module uses hashtable, callbacks or shared state variables provided by the Liberty server to pass authentication data to the system login module.

### About this task

You can use a custom login module to either make additional authentication decisions or add information to the subject to make finer-grained authorization decisions inside your application. See “JAAS configuration” on page 978 and “JAAS login modules” on page 979 for a more detailed overview.

You can also use the developer tools to configure a custom JAAS login module.

**Distributed operating systems**

See “Configuring JAAS on Liberty by using developer tools” on page 1870. **8.5.5.0** There are several security configuration examples on the WASdev.net website for reference when configuring security for your applications on Liberty. See “Configuring JAAS on Liberty by using developer tools” on page 1870.

To configure a JAAS custom login module, complete the following steps:

## Procedure

1. Enable the appSecurity-2.0 Liberty feature in the server.xml file.

```
<featureManager>
  <feature>appSecurity-2.0</feature>
</featureManager>
```

2. Create a class `com.sample.CustomLoginModule` that implements the `LoginModule` interface and package it into the `CustomLoginModule.jar` file.

3. Create a `<library>` element that uses a `<fileset>` element indicating where the `CustomLoginModule.jar` file is. In this example, the library `id` is `customLoginLib`.

```
<library id="customLoginLib">
  <fileset dir="{server.config.dir}" includes="CustomLoginModule.jar"/>
</library>
```

4. Create a `<jaasLoginModule>` element. In this example, the `id` is `custom`.

a. Configure the custom login module to require a successful authentication by setting the `controlFlag` attribute to `REQUIRED`.

b. Set the `libraryRef` attribute to `customLoginLib`, the `id` of the `<library>` element configured in the previous step. This login module also has two options: `UserRegistry` is `ldap` and `mapToUser` is `user1`.

```
<jaasLoginModule id="myCustom"
  className="com.sample.CustomLoginModule"
  controlFlag="REQUIRED" libraryRef="customLoginLib">
  <options myOption1="value1" myOption2="value2"/>
</jaasLoginModule>
```

5. Create a `<jaasLoginContextEntry>` element with an `id` and a unique `name` of the system-defined JAAS configuration: `system.WEB_INBOUND`. You can also set this JAAS configuration to `system.DEFAULT`, `WSLogin`, or your own JAAS configuration. On the `loginModuleRef` attribute, add `custom`, the `id` of the `jaasLoginModule` element created in the previous step. Putting this `id` first in the list means that it is the first JAAS login module to be called. You must also list the other default login modules: `hashtable`, `userNameAndPassword`, `certificate`, and `token`.

```
<jaasLoginContextEntry id="system.WEB_INBOUND" name="system.WEB_INBOUND"
  loginModuleRef="myCustom, hashtable, userNameAndPassword, certificate, token" />
```

**Note:** The option name cannot start with a period (`.`), `config.`, or `service` and must be unique. Also, the property name `id` or `ID` is not allowed.

For more information about the `<jaasLoginContextEntry>`, `<jaasLoginModule>`, `<options>`, and `<library>` elements, see .

## Configuring an application JAAS custom login context entry and login module using a JAAS configuration file for Liberty

8.5.5.9

JAAS configuration information can be configured in a JAAS configuration file.

### About this task

We support the `server.xml` file, `client.xml` file and the JAAS configuration file for JAAS configuration. However, it is suggested to configure the JAAS custom login module in the `server.xml` file or `client.xml` file. For further details about configuring the JAAS custom login module, see “Configuring a JAAS custom login module for Liberty” on page 1868.

The Liberty server reads the JAAS configuration file for an application JAAS custom login context entry and login module. The changes that are made to the JAAS configuration file are used by the local application and take effect after the application server is restarted. The JAAS configuration in the `server.xml` file takes precedence over what is defined in the JAAS configuration file. A configuration entry in the JAAS configuration file is overridden by an entry of the same alias name in the `server.xml` file.

To configure a JAAS custom login module, complete the following steps:

## Procedure

1. Enable the appSecurity-2.0 Liberty feature in the server.xml file.  

```
<featureManager>
  <feature>appSecurity-2.0</feature>
  ...
</featureManager>
```
2. Create a JAAS custom login module class.  
For example, com.sample.CustomLoginModule that implements the LoginModule interface and package it into the CustomLoginModule.jar file.
3. Create the default jaas directory.

### For the server

```
${server.config.dir}/resources/security/jaas
```

### For the client

```
${client.config.dir}/resources/security/jaas
```

**Note:** All JAAS custom login modules that are specified in the JAAS configuration file must place in the default jaas directory.

4. Place the CustomLoginModule.jar file in the default jaas directory.
5. Create a JAAS configuration file.  
For example, create a myJaas.conf file and place it in the \${server.config.dir}/resources/security/jaas directory that has the following content:

```
myCustomLoginContext {
  com.sample.CustomLoginModule required myOption1="value1" myOption2="value2"
};
```

6. Configure the JAAS configuration file using the jvm.options file. For example,  
-Djava.security.auth.login.config=\${server.config.dir}/resources/security/jaas/myJaas.conf

**Note:** We only support the application custom JAAS login module in the JAAS configuration file. Do not put the default system JAAS configuration information in the JAAS configuration file.

**Note:** The JAAS configuration file is not dynamically updated if you made any changes. We strongly recommend configuring the JAAS configuration information in the server.xml file or client.xml file.

## Configuring JAAS on Liberty by using developer tools

### Distributed operating systems

You can configure a JAAS configuration (system.WEB\_INBOUND) with a custom login module for Liberty by editing the configuration. You do not have to configure JAAS unless you want to customize it.

### Before you begin

For a description of the underlying process of configuring a server, and detailed information about specific aspects of server configuration, see “Administering Liberty manually” on page 1564.

**Avoid trouble:** The developer tools creates the reference to a JAAS login module using the loginModuleRef element. You must change it and use the **loginModuleRef** attribute of jaasLoginContextEntry element. There are several security configuration examples on the WASdev.net website for reference when configuring security for your applications on Liberty.

## Procedure

1. Select **JAAS Login Context Entry** and click **Add**, then enter the login module names.

2. Select **JAAS Login Module: myCustom** and configure your custom login module by entering the **ID** and the **Class name**, then click the arrow next to the **Add** button and select **Global Element** to enter the shared library information.
3. Enter the **ID** for the shared library in the pop-up panel and click **OK**.
4. Configure **Name** and **Description** fields for the shared library, then click the arrow next to the **Add** button and select **Child Element** to add a **Fileset** reference as a child element.
5. Configure the **Fileset**. Click **Browse** in the **Base Directory** field and select the directory where the JAR file is located. Then, click **Browse** in the **Includes pattern** field to select your JAR file that contains your custom login module implementation.
6. Optional: If your custom login module needs any options, you can right-click **JAAS Login Module**, select **Add** and then select **login module options**.
7. Save the configuration. You can find the following configuration saved in the `server.xml` file.

```
<jaasLoginContextEntry name="system.WEB_INBOUND" id="system.WEB_INBOUND">
  <loginModuleRef>myCustom, hashtable, userNameAndPassword, certificate, token</loginModuleRef>
</jaasLoginContextEntry>

<jaasLoginModule className="com.sample.CustomLoginModule"
  id="myCustom" libraryRef="customLoginLib">
</jaasLoginModule>

<library id="customLoginLib" name="customLoginLib"
  description="Custom login module shared library">
  <fileset dir="{server.config.dir}" includes="CustomLoginModule.jar"/>
</library>
```

8. **Required:** To make the configuration work, you must change the `jaasLoginContextEntry` element to include the `loginModuleRef` attribute. You must remove the `loginModuleRef` element and add it as an attribute of the `jaasLoginContextEntry` element.

Here is an example of configuration using the `loginModuleRef` attribute.

```
<jaasLoginContextEntry name="system.WEB_INBOUND" id="system.WEB_INBOUND"
  loginModuleRef="myCustom, hashtable, userNameAndPassword, certificate, token" />

<jaasLoginModule className="com.sample.CustomLoginModule"
  id="myCustom" libraryRef="customLoginLib">
</jaasLoginModule>

<library id="customLoginLib" name="customLoginLib"
  description="Custom login module shared library">
  <fileset dir="{server.config.dir}" includes="CustomLoginModule.jar"/>
</library>
```

## Configuring a Java Authentication SPI for Containers (JASPIC) User Feature



8.5.5.6

You can develop a JASPIC provider to authenticate inbound web requests by using the `com.ibm.wsspi.security.jaspi.ProviderService` interface that is provided in the Liberty server.

### About this task

The Java Authentication SPI for Containers specification, JSR 196, defines an interface for authentication providers. In the Liberty server, you must package your JASPIC provider as a user feature. Your feature must implement the `com.ibm.wsspi.security.jaspi.ProviderService` interface.

## Procedure

1. Create an OSGi component that provides a service that implements the `com.ibm.wsspi.security.jaspi.ProviderService` interface.

The `ProviderService` interface defines method, `getAuthProvider`, which the Liberty runtime invokes to retrieve an instance of your JASPIC provider class that implements the `javax.security.auth.message.config.AuthConfigProvider` interface.

The following example uses OSGi declarative services annotations:

```
@package com.mycompany.jaspi;

import java.util.Map;
import javax.security.auth.message.config.AuthConfigFactory;
import javax.security.auth.message.config.AuthConfigProvider;
import org.osgi.service.component.ComponentContext;
import com.mycompany.jaspi.SampleAuthProvider;
import com.ibm.wsspi.security.jaspi.ProviderService;

@Component(service = { ProviderService.class },
           configurationPolicy = ConfigurationPolicy.IGNORE,
           immediate = true,
           property = { "myProviderProperty1=value1",
                       "myProviderProperty2=value2"})
public class SampleJaspiProviderService implements ProviderService {

    Map<String, String> configProps = null;

    // This method called by the Liberty runtime
    // to get an instance of AuthConfigProvider
    @Override
    public AuthConfigProvider getAuthProvider(Map<String, String>
   AuthConfigFactory factory)
    {
        return new SampleAuthProvider(configProps, factory);
    }

    protected void activate(ComponentContext cc) {
        // Read provider config properties here if needed,
        // then pass them to the AuthConfigProvider factory.
        // This example reads the properties from the OSGi
        // component definition.
        configProps = (Map<String, String>) cc.getProperties();
    }

    protected void deactivate(ComponentContext cc) {}
}
```

2. Package the component into an OSGi bundle that is part of your user feature, along with your JASPIC authentication provider.
3. Ensure that your feature includes the OSGi subsystem content: `com.ibm.websphere.appserver.jaspic-1.1; type="osgi.subsystem.feature"`.
4. After the feature is installed into the user product extension location, configure the `server.xml` file with the feature name. For example:

```
<featureManager>
...
<feature>usr:myJaspiProvider</feature>
</featureManager>
```

## Configuring LTPA in Liberty

You can configure a Liberty server to use a specific Lightweight Third Party Authentication (LTPA) keys file, user-defined password, and expiration time.

## About this task

The LTPA is configured by default when security is enabled for a Liberty server for the first time. The default location of the automatically generated LTPA keys file is `${server.output.dir}/resources/security/ltpa.keys`. The LTPA keys are encrypted with a randomly generated key and a default password of WebAS is initially used to protect the keys. The password is required when importing the LTPA keys into another server. To protect the security of the LTPA keys, you must change the password. When the LTPA keys are exchanged between servers, this password must match across the servers for Single Sign On (SSO) to work.

The default expiration timeout is 120 minutes. The expiration value refers to how long the LTPA tokens are valid before they expire.

**8.5.0.1** To enable dynamic reloading of the LTPA keys when copying an LTPA keys file from another server, you can specify a file monitor interval before copying the LTPA keys file. The monitor interval value refers to how often the LTPA keys file is monitored for updates.

For more information about LTPA, see LTPA concept in Liberty.

## Procedure

1. Configure the `<ltpa>` element in the `server.xml` file as follows, replacing the sample values in the example with your values:

```
<ltpa keysFileName="yourLTPAKeysFileName.keys" keysPassword="keysPassword" expiration="120" />
```

2. **8.5.0.1** Optional: Set the **monitorInterval** attribute to check the `ltpa.keys` file for key changes to be dynamically reloaded. Specify a positive integer followed by a unit of time, which can be hours (h), minutes (m), or seconds (s). In the following example, the LTPA keys file is checked for changes to be dynamically reloaded every 5 seconds:

```
<ltpa keysFileName="yourLTPAKeysFileName.keys" keysPassword="keysPassword"
      expiration="120" monitorInterval="5s" />
```

3. Encode the password within the configuration. You can get the encoded value by using the `securityUtility encode` command.
4. **8.5.0.1** Optional: Copy an existing LTPA keys file to the location specified in the **keysFileName** attribute. The default value is `${server.output.dir}/resources/security/ltpa.keys`. **8.5.0.1**  
For more information on `<ltpa>` element, see .

## OpenID



8.5.5.4

OpenID is an open standard where users can authenticate themselves to multiple entities without the need to manage multiple accounts or sets of credentials. WebSphere Application Server Liberty supports OpenID 2.0 and plays a role as a Relying Party in web single-sign-on.

### OpenID Provider (OP)

An OpenID Authentication server that can assert whether a user controls a unique identifier.

### Relying Party (RP)

An entity that requires proof that a user controls a unique identifier.

### OpenID Identifier:

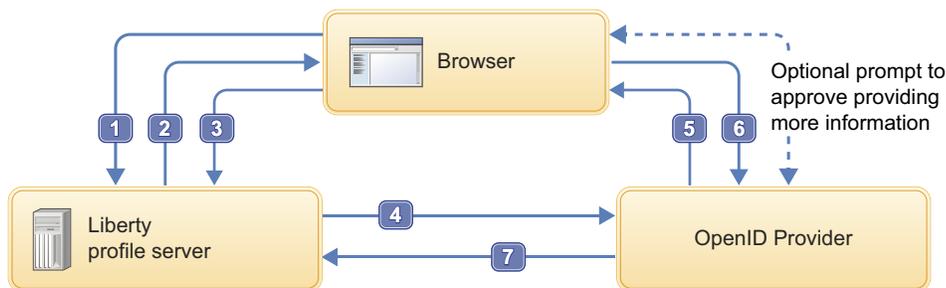
An http or https URL that belongs to an OpenID provider or a user.

Accessing various entities such as websites often requires a unique account that is associated with each entity. OpenID enables a single set of credentials that are handled by an OpenID Provider to grant access to any number of entities that support OpenID.

When required to sign in to an entity, such as a website that supports OpenID and acts as a Relying Party, users perform authentication by interacting directly with an OP rather than providing their credentials to the RP itself. An OP verifies the identity of the user and sends an authentication confirmation back to the RP. When this confirmation is received from the OP, the RP accepts the user as authenticated.

A typical OpenID authentication flow is described as follows:

1. A user attempts to access a protected resource, such as a web page.
2. The Liberty server, acting as a RP, presents a form login page for the protected resource.
3. The user enters an OpenID identifier.
4. The RP takes the identifier and redirects the user to the appropriate OP.
5. The OP prompts the user for credentials.
6. The user enters credentials for the account that is associated with the OP.
7. The OP authenticates the user and optionally prompts the user to approve or deny providing user information to the RP, and subsequently redirects the user back to the RP with the authentication result.
8. If the OP authentication is successful, the RP attempts to authorize the user.
9. If the user authorization is successful, the RP establishes an authenticated session with the user.



OpenID helps minimize the chances of user credentials or sensitive information being mishandled. With OpenID, a user's credentials are only exchanged with the OpenID Provider, meaning no website other than the OP ever sees the user's credentials. This standard helps mitigate the possibility of an unscrupulous or insecure website compromising the identity of a user. The user also controls how much personal information is shared with the websites visited. For example, users can choose to allow the name and email address that are associated with their OpenID account to be shared with one website while electing not to provide their email address, or any information at all, to another website.

The OpenID standard specifications that are supported include:

OpenID Authentication 2.0.

OpenID Attribute Exchange 1.0.

**Note:** The OpenID 2.0 Claimed Identifier should be used to identify a user per spec, Identifying the end user. However, the Claimed Identifier is not user friendly and many Relying Parties choose one of the OpenID attributes to represent the user. The most popular attribute used to represent the user is a user's email address.

It is known that some OpenID attributes, including email, might not be validated by the OpenID provider. If you do not trust that a provider will provide you a verified email address, then you must not use the provider's email as the authenticated user name in the WebSphere Application Server.

## OpenID Connect



8.5.5.4

OpenID Connect is a simple identity protocol and open standard that is built on top of the OAuth 2.0 protocol that enables client applications to rely on authentication that is performed by an OpenID Connect Provider to verify the identity of a user.

OpenID Connect uses OAuth 2.0 for authentication and authorization and then builds identities that uniquely identify users. Client applications can also obtain basic profile information about a user in an interoperable and REST-like manner from OpenID Connect Providers.

The WebSphere Application Server Liberty supports OpenID Connect 1.0 and plays a role as a Client, or Relying Party, and as a Provider in web single sign-on. The following OpenID Connect specification is supported:



8.5.5.4

OpenID Connect Core 1.0

For those using a Liberty server as a Web-based Relying Party, the 

8.5.5.4

 OpenID Connect Basic Client Implementer's Guide 1.0 is a subset of the OpenID Connect Core specification that is easier to read and provides details for Web-based Relying Parties that use the Authorization Code Flow.

### Access Token

A credential that is used to access protected resources. An access token is a string that represents an authorization that is issued to the client.

### Authorization Endpoint

A resource on an OpenID Provider that accepts an authorization request from a client to perform authentication and authorization of a user. The authorization endpoint returns an authorization grant, or code, to the client in the Authorization Code Flow. In the Implicit Flow, the authorization endpoint returns an ID token and access token to the client.

### Authorization Grant

A credential that represents a user's authorization to access resources, and is used by a client to obtain an access token.

**Claim** Information asserted about an entity. Examples of a claim include phone number, first name, last name, and others.

### ID Token

JSON Web Token (JWT) that contains claims about the authenticated user.

### Introspection Endpoint

A resource on an OpenID Provider that enables a client that is holding an access token to retrieve information that was used to create the access token, such as the user name, granted scopes, client ID, or other information.

### OpenID Connect Provider (OP)

An OAuth 2.0 authorization server that is capable of providing claims to a client, or Relying Party (RP).

### Refresh Token

Issued to the client by the OP and is used to obtain a new access token when the current access token expires, or to obtain more access tokens.

**Relying Party (RP)**

Either a Liberty server configured as an OpenID Connect Client, or a client application that requires claims from an OpenID Provider (OP).

**Scope** Privilege or permission that is allowed to access resources of a third party.

**Token Endpoint**

A resource on an OP that accepts an authorization grant, or code, from a client in exchange for an access token, ID token, and refresh token.

**The Liberty server as an OpenID Connect Client**

You can configure the WebSphere Application Server Liberty to function as an OpenID Connect Client. This setup enables the Liberty server to rely on another Liberty server that is acting as an OP for user authentication and authorization.

A Liberty server that is configured to act as an OpenID Connect Client supports the Authorization Code Flow of the OpenID Connect 1.0 standard.

In the Authorization Code Flow, all token exchanges are handled by using the token endpoint of the OpenID Connect Provider. First, the client submits an authorization request to the authorization endpoint of the OP. Upon successful authentication and authorization with the OP, the client receives an authorization grant, or code, from the OP. This authorization code can then be sent in a request to the token endpoint of the OP. The client receives an ID token, an access token, and a refresh token in the response from the token endpoint. The client then validates the ID token and retrieves the subject identifier of the user. This profile flow is intended for clients that can securely maintain a client secret between themselves and the OP. This flow also allows clients to obtain a refresh token.

For configuring a Liberty server as an OpenID Connect Client, see “Configuring an OpenID Connect Client in Liberty” on page 1924

**The Liberty server as an OpenID Connect Provider**

You can configure the WebSphere Application Server Liberty to function as an OpenID Connect Provider. This setup enables the Liberty server to act as an authorization server that can be used by OpenID Connect Clients.

A Liberty server that is configured to act as an OpenID Connect Provider supports the Authorization Code Flow and Implicit Flow of the OpenID Connect 1.0 standard. Each flow determines how the ID token, access token, and refresh token are returned to the client.

The Authorization Code Flow handles all token exchanges by using the token endpoint of the OpenID Connect Provider. An OpenID Connect Provider accepts an authorization request from a client at the OP's authorization endpoint. If authentication is necessary, the OpenID Connect Provider performs the appropriate authentication. The OpenID Connect Provider also obtains any required consent or authorization from the user, for example by prompting the user in a browser for permission to grant access to certain scopes. If successful, or if no authentication was required, the OpenID Provider sends back an authorization grant, or code, to the client. The OpenID Connect Provider then accepts a request that is submitted to its token endpoint by the client that includes the authorization code. The request that includes the authorization code is validated by the OpenID Provider. Upon successful validation, the OpenID Connect Provider returns a response to the client that includes an ID token and an access token.

In the Implicit Flow, unlike the Authorization Code Flow, all tokens are returned from the authorization endpoint; the token endpoint of the OP is not used. First, a client prepares and sends an authentication request to the authorization endpoint of the OP. The OpenID Connect Provider then performs any necessary authentication and also obtains any required consent or authorization from the user. For example, the OpenID Connect Provider prompts the user in a browser for permission to grant access to

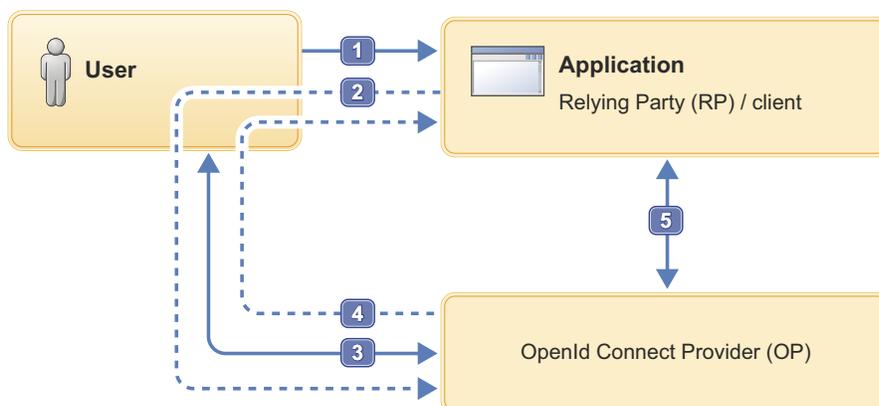
certain scopes. Upon successful authentication and authorization, the OpenID Connect Provider sends back an ID token and an access token to the client. The client then validates the ID token and retrieves the subject identifier of the user. This profile flow is intended for clients that cannot securely maintain a client secret between themselves and the OP, such as native applications.

For configuring a Liberty server as an OpenID Connect Provider, see “Configuring an OpenID Connect Provider in Liberty” on page 1899

## Authorization Code Flow

A typical OpenID Connect Authorization Code Flow is described as follows:

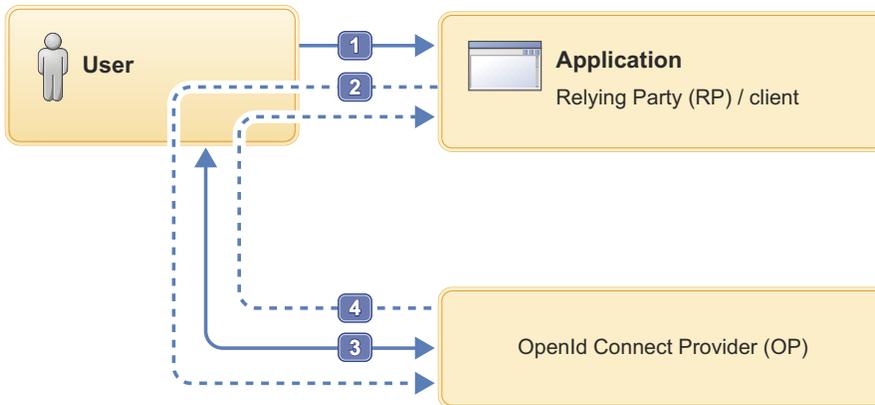
1. A user accesses an application on the RP.
2. The RP prepares an authentication request and redirects the user to the OP.
3. The OP authenticates the user, for example by prompting the user for credentials. The user authorizes the RP to access the information that is required by the application. The OP generates a one-time use authorization code for the RP.
4. The OP redirects the user back to the RP with the authorization code.
5. The RP calls the token endpoint of the OP to exchange the authorization code for an access token, ID token, and a refresh token.
6. The RP uses the ID token to authorize the user.



## Implicit Flow

The Implicit Flow is only supported by Liberty servers that are acting as an OpenID Connect Provider. A typical OpenID Connect Implicit Flow is described as follows:

1. A user accesses an application on the RP.
2. The RP prepares an authentication request and redirects the user to the OP.
3. The OP authenticates the user, for example by prompting the user for credentials. The user authorizes the RP to access the information that is required by the application.
4. The OP redirects the user back to the RP with an ID token and an access token.
5. The RP uses the ID token to authorize the user.



## Configuring an OpenID Relying Party in Liberty



8.5.5.4

You can configure a Liberty server to function as an OpenID Relying Party to take advantage of web single-sign-on.

### Before you begin

You must have at least one OpenID Provider (OP) that is trusted with authenticating users. Several third-party OpenID Providers are available.

### About this task

You can have users authenticated with an OpenID Provider by enabling the `openid-2.0` feature in Liberty, and in addition to other optional configuration information.

### Procedure

1. Add the `openid-2.0` Liberty feature to the `server.xml` file. Add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>openid-2.0</feature>
```

2.  Update the `server.xml` file with the OpenID Relying Party configuration options that are specified by an `<openId>` element.

You can either predefine an OpenID provider URL in your `server.xml` file by using the **providerIdentifier** attribute of the `<openId>` element, or you can package your application with `FormLogin` which gives users an option to submit an OpenID provider URL to use for authentication.

If the **providerIdentifier** attribute is added to the `server.xml` file, the Liberty server will automatically redirect users to the OpenID provider specified by that attribute. If the **providerIdentifier** attribute is not defined in the `server.xml` file, the Liberty server will first send a login form to ask the user to select or confirm an OpenID provider prior to redirecting the user to the OpenID provider.

The following is a sample OpenID configuration that defines an OpenID provider:

```
<openId id="myOpenId" providerIdentifier="https://openid.acme.com/op" userInfoRef="email">
  <userInfo id="email" alias="email" uriType="http://axschema.org/contact/email" count="1" required="true" />
</openId>
```

Adding the `openid-2.0` feature automatically enforces a certain minimum configuration. Consequently, there is no `<openId>` element that is required to be explicitly specified in the `server.xml` file. Without an `<openId>` element that is specified, the following configuration is implicit:

```
<openId id="myOpenId" userInfoRef="email">
  <userInfo id="email" alias="email" uriType="http://axschema.org/contact/email" count="1" required="true" />
</openId>
```

By default, the user's email address that is returned from the OpenID Provider is used for identity assertion and subject creation.

3. Configure the server's truststore to include the signer certificates of the OpenID Providers that are supported. For information about keystores, see [Enabling SSL communication for Liberty](#).
  - a. Extract the signer certificate from the OpenID Provider. Most major web browsers provide support for extracting or exporting certificates from websites through the browser interface.
  - b. Import the OpenID Provider certificate to the server's truststore. For one method of importing certificates into a truststore, see the `-import` flag capabilities of the **keytool** utility that is found in your Java installation directory.
  - c. Use the `sslRef` attribute of the `<openId>` element to point to your SSL configuration. If no `sslRef` attribute is specified, the default SSL configuration described in the keystore page mentioned previously will be used. Your SSL configuration should include the appropriate references to the truststore containing the imported OpenID Provider certificates.

4. Optional: Configure the Authentication Filter.

If the `providerIdentifier` attribute is configured inside the `openId` element in the `server.xml` file, you can configure `authFilterRef` to limit the requests that should be intercepted by the OpenID provider defined by the `providerIdentifier` attribute.

For more information on configuring the authentication filter, see  [8.5.5.5](#) “Authentication Filters” on page 1937.

## Configuring SPNEGO authentication in Liberty



8.5.5.5

You can use single sign-on for HTTP requests by using the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) web authentication for WebSphere Application Server Liberty. SPNEGO single sign-on enables HTTP users to log in to a Microsoft® domain controller only once at their desktop and to achieve single sign-on (SSO) with the Liberty server.

### Before you begin

Configure the following software and ensure that it is available:

1. A Microsoft Windows® Server running an Active Directory Domain Controller and associated Kerberos Key Distribution Center (KDC). For this topic, an example host for such a domain controller is `myAdMachine.example.com`. The domain controller name is `mydomain.example.com` and the Kerberos realm name is `MYDOMAIN.EXAMPLE.COM`, which is the domain controller name in all uppercase letters.
2. A Microsoft Windows® domain member (client) that supports the SPNEGO authentication mechanism as defined in IETF RFC 2478. Examples of an appropriate client might be a modern browser or a Microsoft .NET client. Most modern browsers support SPNEGO authentication. For this topic, an example host for the client is `myClientMachine.example.com`.
3. A server platform with a Liberty server that has a protected resource within an application. Users in the Active Directory must be able to access Liberty server protected resources by using a native Liberty server authentication mechanism. For this topic, an example Liberty server host is `myLibertyMachine.example.com`.

**Note:** The software configuration must have a running domain controller, at least one client machine in that domain and a server platform with a Liberty server that has a protected resource within an application, for a total of three required machines. Using SPNEGO directly from the domain controller is not supported.

**Note:** Ensure the clocks for the client, Microsoft Active Directory server, and Liberty server are synchronized to within 5 minutes of each other, by default. The allowable difference in synchronization is configurable.

**Note:** Only IBM JDKs are supported currently. Non-IBM JDKs are not supported.

## About this task

The objective of this task is to allow users to successfully access Liberty server resources without having to authenticate again, and thus achieve Microsoft Windows® desktop single sign-on capability.

This task demonstrates how to configure a Liberty server to support single sign-on for HTTP requests by using SPNEGO web authentication.

## Procedure

1. On the Microsoft domain controller (myAdMachine.example.com), create a Kerberos service principal name (SPN) and keytab file for the Liberty server. :
  - a. Create a user account for the Liberty server. This is the account that is used to map to the Kerberos service principal name (SPN). For Active Directory machines, this can typically be done by going to **Start > Administrative Tools > Active Directory Users and Computers**, right-clicking on **Users** in the panel, and selecting **New > User**. This topic assumes that the user myLibertyMachine\_http was created with password security.
  - b. Run the Microsoft **setspn** command to map the user account to a Kerberos SPN. This user account represents the Liberty server as being a Kerberos service with the KDC. The following is an example **setspn** command:

```
C:\> setspn -a HTTP/myLibertyMachine.example.com myLibertyMachine_http
```

```
Registering ServicePrincipalNames for CN=myLibertyMachine_http,CN=Users,DC=MYDOMAIN,DC=EXAMPLE,DC=COM
HTTP/myLibertyMachine.example.com
Updated object
```

**Note:** If your Microsoft **setspn** command version supports the **-S** option, then you must use the **-S** option instead of **-A**.

- c. Create the Kerberos keytab file by using the Microsoft **ktpass** tool. The default name for this file is krb5.keytab.

The following is an example **ktpass** command:

```
C:\> ktpass -out krb5.keytab -princ HTTP/myLibertyMachine.example.com@MYDOMAIN.EXAMPLE.COM -mapUser myLibertyMachine
```

```
Targeting domain controller: myAdMachine.MYDOMAIN.EXAMPLE.COM
Using legacy password setting method
Successfully mapped HTTP/myLibertyMachine.example.com to myLibertyMachine_http.
Key created.
Output keytab to krb5.keytab:
Keytab version: 0x502
keysize 93 HTTP/myLibertyMachine.example.com@MYDOMAIN.EXAMPLE.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (
```

Make sure that there is not a duplicated SPN in the Microsoft forest by using one of the following commands:

- If your Microsoft **setspn** command version supports the **-X** option to search for a duplicated SPN, then use **setspn -X**:

```
C:\>setspn -X HTTP/myLibertyMachine.example.com
```

```
Processing entry 0
found 0 group of duplicate SPNs.
```

- You can also use the Microsoft **ldif** command. The following example shows that one entry was returned, meaning there is not a duplicated SPN.

```
C:\>ldifde -f check_SPN.txt -t 3268 -d "" -l servicePrincipalName -r "(servicePrincipalName=HTTP/myLibertyMachine.example.com)" -p subtree
```

```
Connecting to "myAdMachine.MYDOMAIN.EXAMPLE.COM"  
Logging in as current user using SSPI  
Exporting directory to file check_SPN.txt  
Searching for entries...  
Writing out entries.  
1 entries exported
```

For information on creating SPNs and keytab files on different KDC systems, see [Creating a Kerberos service principal name and keytab file](#).

2. On the Liberty server machine (myLibertyMachine.example.com), enable the Kerberos keytab and configuration files and SPNEGO web authentication.
  - a. Copy the Kerberos keytab file from the domain controller to the Liberty server machine. The default name of this file is krb5.keytab and the default location varies depending on the platform but is the same directory as the Kerberos configuration file. For default locations for various platforms, see the next step.
  - b. Create a Kerberos configuration file.

The Kerberos configuration file contains client configuration information, including the locations of KDCs for the realms of interest, defaults for the current Kerberos realm, and mappings of host names onto Kerberos realms. For Liberty servers, you must create this file manually.

The default location and name of this file varies depending on the operating system:

- **Windows** Windows - The default location is c:\winnt\krb5.ini. If the krb5.ini file is not in the c:\winnt directory, it might be in c:\windows
- **Linux** Linux - The default location is /etc/krb5.conf.
- **AIX** **z/OS** **HP-UX** **Solaris** AIX, z/OS, HP-UX, and Solaris - The default location is /etc/krb5/krb5.conf.

The following is a sample Kerberos configuration file for the AIX, z/OS, HP-UX, or Solaris platforms (based on the default keytab location):

```
[libdefaults]  
    default_realm = MYDOMAIN.EXAMPLE.COM  
    default_keytab_name = FILE:/etc/krb5/krb5.keytab  
    default_tkt_enctypes = rc4-hmac  
    default_tgs_enctypes = rc4-hmac  
    forwardable = true  
    renewable = true  
    noaddresses = true  
    clockskew = 300  
    udp_preference_limit = 1  
[realms]  
    MYDOMAIN.EXAMPLE.COM = {  
        kdc = myAdMachine.example.com:88  
        default_domain = example.com  
    }  
[domain_realm]  
    .example.com = MYDOMAIN.EXAMPLE.COM
```

**Note:** Realm names are usually specified in uppercase letters. If using Microsoft Active Directory, realm names are required to be uppercase.

**Note:** Not all of the KDC solutions available support all encryption types. Before choosing an encryption type, ensure that the KDC supports the encryption type that you want to use by consulting your Kerberos Administrator's and User's Guide.

Ensure that you have a common encryption type for the Kerberos configuration file, Kerberos keytab file, Kerberos SPN, and Kerberos client. For example, if the Kerberos client uses the

RC4-HMAC encryption type, the target server must also support the RC4-HMAC encryption type and the Kerberos configuration file must list RC4-HMAC first in the **default\_tgt\_encytypes** and **default\_tkt\_encytypes** parameters.

For additional information and requirements on the content of this file, see *Creating a Kerberos configuration file*.

c. Verify the Kerberos configuration and keytab files.

- You can use the JDK command **klist** to list the SPN in the keytab file.

```
klist -k -t /etc/krb5.keytab
```

- You can use the JDK command **kinit** to validate the SPN in the keytab file and the Kerberos configuration file.

```
kinit -k -t /etc/krb5.keytab HTTP/myLibertyMachine.example.com
```

After the **kinit** command you can use the **klist** command to list the Kerberos ticket. If you get the Kerberos ticket, then the Kerberos keytab and configuration are valid.

d. Configure and enable SPNEGO web authentication on the Liberty server.

You can enable SPNEGO web authentication by enabling the `spnego-1.0` feature of the Liberty profile.

1) Add the `spnego-1.0` feature to the `server.xml` file.

```
<featureManager>
  <feature>spnego-1.0</feature>
  <feature>appSecurity-2.0</feature>
  ...
</featureManager>
```

Adding the `spnego-1.0` feature automatically enforces a certain minimum configuration. You do not need to specify a `<spnego>` element in the `server.xml` file. Without specifying a `<spnego>` element, the following configuration is implicit.

```
<spnego
  canonicalHostName="true"
  disableFailOverToAppAuthType="true"
  trimKerberosRealmNameFromPrincipal="true"
  includeClientGSSCredentialInSubject="true" />
```

**Note:** The runtime forms the default SPN in the following format:

```
"HTTP/" + java.net.InetAddress.getLocalHost().getCanonicalHostName();
```

If the default SPN does not match what you have in the `krb5.keytab` file, then you need to specify the `servicePrincipalNames`, for example:

```
<spnego id="mySpnego" servicePrincipalNames="HTTP/myLibertyMachine.example.com"/>
```

**Note:** When the `spnego-1.0` feature is enabled and the `<spnego>` element is either omitted or not configured with an `authFilterRef` attribute, all requests to access protected resources use SPNEGO authentication.

For more information on configuring the authentication filter, see  **8.5.5.5** “Authentication Filters” on page 1937.

**Note:** When values for the `krb5Config` or `krb5Keytab` attributes are not given, each respective file is expected to exist at its default location. The default locations for the Kerberos configuration and keytab files on various platforms are given earlier in this topic.

2) Optional: Specify any additional configuration options as necessary. Liberty supports many common SPNEGO scenarios and configurations. For example, you can filter HTTP requests to require SPNEGO authentication for only certain requests, web applications, hosts, or user agents. Also, you can move the Kerberos configuration and keytab files away from their respective default locations. The following is a sample configuration that changes the default `<spnego>` settings:

```

<server>
  <featureManager>
    <feature>spnego-1.0</feature>
    <feature>appSecurity-2.0</feature>
    ...
  </featureManager>
  ...
  <authFilter id="myAuthFilter">
    <host id="myHost" name="example.com" matchType="contains" />
    <webApp id="myWebApp" name="protectedApp" matchType="equals" />
  </authFilter>

  <spnego id="mySpnego"
    includeClientGSSCredentialInSubject="false"
    krb5Config="${server.config.dir}/resources/security/kerberos/krb5.conf"
    krb5Keytab="${server.config.dir}/resources/security/kerberos/krb5.keytab"
    servicePrincipalNames="HTTP/myLibertyMachine.example.com"
    authFilterRef="myAuthFilter" />
  </spnego>
  ...
</server>

```

With this configuration, SPNEGO authentication is used for any requests that are received containing the host name `example.com` for resources within the web application `protectedApp`. In addition, the client's GSS credentials are not added to the user subject upon successful authentication. Finally, the Kerberos configuration and keytab files to be used by the server are given specific locations within the server configuration directory instead of their respective default locations.

For more configuration options, see  [8.5.5.5](#) The Simple and Protected GSS-API Negotiation Mechanism (SPNEGO).

For information on mapping Kerberos principal names to WebSphere user registry IDs, see Mapping of a client Kerberos principal name to the WebSphere user registry ID.

In the rare event that you wish to use Kerberos principal names for authorization, see  [8.5.5.5](#) "Using Kerberos principal name for authorization with SPNEGO authentication" on page 1886. These steps should be followed only when necessary and by users who specifically choose not to use the default mapping or JAAS custom login module mapping.

3. Configure the client application on the client application machine (`myClientMachine.example.com`).

The following steps must be done only on the client machine. Starting a browser on the Active Directory machine or Liberty server machine and performing these steps does not work.

The following steps are for users who are accessing SPNEGO-protected resources from a browser. You must have a browser installed that supports SPNEGO authentication.

Microsoft Internet Explorer:

- a. At the desktop, log in to the Windows Active Directory domain.
- b. In the Internet Explorer window, click **Tools > Internet Options**. In the window that is displayed, click the **Security** tab.
- c. Select the **Local intranet** icon and click **Sites**.
- d. If using Internet Explorer version 9 or older, go to the next step. If using Internet Explorer 10 or later, click **Advanced** in the Local intranet window.
- e. In the Local intranet window, complete the **Add this website to the zone** field with the web address of the host name so that single sign-on (SSO) can be enabled for the list of websites that are shown in the websites field. Your site information technology staff provides this information. Close the second Local intranet window and click **OK** to complete this step and close the Local intranet window.
- f. On the Internet Options window, click the **Advanced** tab and scroll to Security settings. Ensure that the **Enable Integrated Windows® Authentication** box is selected.
- g. Click **OK**. Restart your Microsoft Internet Explorer to activate this configuration.

Mozilla Firefox:

- a. At the desktop, log in to the Windows Active Directory domain.
- b. In the address field in Firefox, type `about:config`.
- c. In the Filter/Search box, type `network.n`.
- d. Double-click **network.negotiate-auth.trusted-uris**. This preference lists the sites that are permitted to engage in SPNEGO Authentication with the browser. Enter a comma-delimited list of trusted domains or URLs.

**Note:** You must set the value for `network.negotiate-auth.trusted-uris`.

- e. If the deployed SPNEGO solution is using the advanced Kerberos feature of Credential Delegation, double-click **network.negotiate-auth.delegation-uris**. This preference lists the sites for which the browser can delegate user authorization to the server. Enter a comma-delimited list of trusted domains or URLs.
- f. Click **OK**. The configuration reflects the updates.
- g. Restart your Firefox browser to activate this configuration.

**Note:** The user must be logged in to the domain controller for SPNEGO to work. Using the previous example machines, a user must log in to the domain controller at `MYDOMAIN.EXAMPLE.COM\username` in order for SPNEGO authentication through the browser to work.

**Note:** If you are prompted multiple times for a user ID and password, make sure that you enabled SPNEGO support on your client browser by following the previous instructions. You must also make sure that the `disableFailOverToAppAuthType` attribute in the `<spnego>` configuration is set to `false`.

## Results

Your Internet browser is now properly configured for SPNEGO authentication. You can use applications with secured resources that are deployed on Liberty servers without being prompted for a user ID and password.

To verify that SPNEGO is working, you can log in to the domain controller and then access a protected resource on the Liberty server, and because you are logged in to the domain controller, you are not prompted for credentials. However, if you do not log in to the domain controller and attempt to access a protected resource, you are prompted for credentials.

## Configuring Kerberos constrained delegation for out-bound SPNEGO tokens in Liberty

You can configure a Liberty server to support Kerberos constrained delegation for out-bound SPNEGO tokens.

### Before you begin

Make sure that you have configured SPNEGO web authentication.

Only IBM JDK 1.8 and later are supported.

### About this task

The Kerberos v5 extension called S4U (Services for Users) also known as constrained delegation comprises two parts:

**S4U2self**

Allows a Liberty server to obtain a service ticket to itself on behalf of a user. This can be used with any form of authentication that is supported by Liberty. S4U2self is the Kerberos Protocol Transition extension.

### S4U2proxy

Allows a Liberty server to obtain service tickets to trusted services on behalf of a user. These service tickets are obtained by using the user's service ticket to the Liberty service. The services are constrained by the Kerberos Key Distribution Center (KDC) administrator. S4U2proxy is the Kerberos Constrained Delegation extension.

The constrained delegation feature provides the following APIs to create the out-bound SPNEGO token for back end services that support SPNEGO authentication, such as .NET servers and other Liberty servers.

- S4U2self API:  
`com.ibm.websphere.security.s4u2proxy.SpnegoHelper.buildS4U2proxyAuthorizationUsingS4U2self()`
- S4U2proxy API:  
`com.ibm.websphere.security.s4u2proxy.SpnegoHelper.buildS4U2proxyAuthorization()`

The following steps use the same example system setup that is used in Configuring SPNEGO authentication in Liberty and illustrated in Single sign-on for HTTP requests using SPNEGO web authentication.

### Procedure

1. On the Microsoft domain controller `myAdMachine.example.com`, update the service principal name (SPN) that you use to validate the incoming SPNEGO token. For example, update the `HTTP/myLibertyMachine.example.com` SPN as follows:
  - a. To use S4U2self, perform the following steps:
    - 1) Open the user account that is mapped to the delegate SPN.
    - 2) Open the Attribute Editor tab.
    - 3) Modify the `userAccountControl` property as follows:
      - Trusted for auth delegation `0x1000000`, or the `TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION` enum) must be true.
    - 4) Set the trusted service:
      - Open the Delegation tab in the user account.
      - Select the **Trust this user for delegation to specified services only** radio button.
      - Select the **Use any authentication protocol** radio button.
      - Click on **Add** to add the trusted service.
      - Click **Users or Computers**.
      - Enter the SPN to be used for the trusted service.
      - Click **Check Names** and verify that the appropriate object name was found.
      - Click **OK**.
      - Select the **SPN specified** and click **OK**.
  - b. To use S4U2proxy, perform the following steps:
    - 1) Open the user account that is mapped to the delegate SPN.
    - 2) Open the Attribute Editor tab.
    - 3) Modify the `userAccountControl` property as follows:
      - Trusted for auth delegation (`0x1000000`, or the `TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION` enum) must be true.
    - 4) Set the trusted service:
      - Open the Delegation tab in the user account.

- Select the **Trust this user for delegation to specified services only** radio button.
  - Click on **Add** to add the trusted service.
  - Click **Users or Computers**.
  - Enter the SPN to be used for the trusted service.
  - Click **Check Names** and verify that the appropriate object name was found.
  - Click **OK**.
  - Select the **SPN specified** and click **OK**.
2. On the Liberty server machine (myLibertyMachine.example.com), enable the constrained delegation feature by adding constrainedDelegation-1.0 to the featureManager and configure the JAAS Kerberos login module in the server.xml file.

```
<featureManager>
  <feature>spnego-1.0</feature>
  <feature>constrainedDelegation-1.0</feature>
  ...
</featureManager>
<jaasLoginContextEntry id="com.ibm.security.jgss.krb5.accept" name="com.ibm.security.jgss.krb5.accept" loginModuleRef="U
  <jaasLoginModule id="useKeytab" className="com.ibm.security.auth.module.Krb5LoginModule" controlFlag="REQUIRED" libra
    <options
      credsType="both"
      debug="true"
      useDefaultCcache="false"
      tryFirstPass="true"
      forwardable ="true"
      principal="HTTP/myLibertyMachine.example.com"
      useKeytab="${server.config.dir}/resources/security/kerberos/krb5.keytab">
    </options>
  </jaasLoginModule>
```

```
<library id="jaasSharedLib" apiTypeVisibility="spec, ibm-api, api">
  <fileset dir="${server.config.dir}/lib/global/" includes="*" />
</library>
```

When the constrainedDelegation-1.0 feature is enabled, the following configuration is implicit:

```
<constrainedDelegation id="defaultConstrainedDelegation" s4U2selfEnabled="false" />
```

To use S4U2self, the following configuration is needed in the server.xml file:

```
<constrainedDelegation s4U2selfEnabled = "true" id="defaultConstrainedDelegation"/>
```

**Note:** When you use the S4U2proxy API, the jaasLoginContextEntry id and name com.ibm.security.jgss.krb5.accept can not change.

**Note:** By default, S4U2proxy is enabled and S4U2self is disabled. The S4U2self extension can be enabled or disabled by modifying the s4U2selfEnabled attribute in the server.xml file.

## Results

Your application is now ready to call the API provided by the constrained delegation feature.

## Using Kerberos principal name for authorization with SPNEGO authentication



8.5.5.5

You can use the fully qualified Kerberos principal name for authorization instead of using simple mapping or creating your own custom JAAS custom login module.

## About this task

The following steps should be rarely followed, and only by users who specifically choose not to use simple mapping, which is the default configuration, or choose not to add a JAAS custom login module to map the fully qualified Kerberos principal name to a user in the Liberty server user registry. This task allows you to use the fully qualified Kerberos principal name for authorization.

## Procedure

1. Configure the SPNEGO authentication to not trim the Kerberos realm name from the fully qualified Kerberos principal name by setting the `trimKerberosRealmNameFromPrincipal` attribute to `false`.
2. Configure the Liberty server to use either stand-alone LDAP or federated repositories.  
For more information on how to configure LDAP, see [Configuring LDAP user registries with Liberty](#).
  - a. Make sure that the Active Directory user exists in the LDAP user registry and that this user has a `userPrincipalName` attribute that is associated with it.
  - b. Update the LDAP filter in the `server.xml` file to search for the `userPrincipalName`, as shown in the following example:

```
<activatedLdapFilterProperties id="myactivatedfilters"
  userFilter="(&(userPrincipalName=%v))"
  groupFilter="(&(cn=%v))"
  userIdMap="*:userPrincipalName"
  groupIdMap="*:cn"
  groupMemberIdMap="ibm-allGroups:member">
</activatedLdapFilterProperties>
```

3. Configure the application bindings for the corresponding application to use the fully qualified Kerberos principal name as the user name along with a properly configured `access-id`. For example:

```
<application type="war" id="myApp" name="myApp" location="{server.config.dir}/apps/myApp.war">
  <application-bnd>
    <security-role name="Employee">
      <user name="kevin@MYDOMAIN.EXAMPLE.COM" access-id="CN=kevin,CN=Users,DC=MYDOMAIN,DC=EXAMPLE,DC=COM"/>
      ...
    </security-role>
    ...
  </application-bnd>
</application>
```

## Customizing SSO configuration using LTPA cookies in Liberty

With single sign-on (SSO) configuration support, web users can authenticate once when accessing Liberty resources such as HTML, JavaServer Pages (JSP) files, and servlets, or accessing resources in multiple Liberty servers that share the same Lightweight Third Party Authentication (LTPA) keys.

### Example

When a user passes authentication on one of Liberty servers, authentication information generated by the server is transported to the web browser in a cookie. The cookie is used to propagate the authentication information to other Liberty servers.

The LTPA is configured and ready for immediate use. The default cookie name used to store the SSO token is called `ltpaToken2`. If you want to use a different name for the cookie, you can customize the cookie name using the `ssoCookieName` attribute of the `<webAppSecurity>` element. If you customize the cookie name, make sure that all the servers that participate in SSO use the same cookie name.

For more information about SSO, see [SSO concept in Liberty](#).

The following example code sets the user to be logged out after the HTTP session expires and the name of the SSO cookie as `myCookieName`:

```
<webAppSecurity logoutOnHttpSessionExpire="true" ssoCookieName="myCookieName" />
```

**Note:** For SSO to work across Liberty servers, full profile servers, or both, set the following resources:

- The servers must use the same LTPA keys and share the same user registry.
- If the servers are not in the same domain, use the **ssoDomainNames** attribute of the <webAppSecurity> element to list the domains. The following example code sets the domain name to domain.com:  

```
<webAppSecurity ssoDomainNames="domain.com" />
```
- If the servers are in the same domain, set the **ssoUseDomainFromURL** attribute of the <webAppSecurity> element to true, or specify the domain name in the **ssoDomainNames** attribute. The following example code sets **ssoUseDomainFromURL** to true so that the domain name is taken from the request URL:  

```
<webAppSecurity ssoUseDomainFromURL="true" />
```

For details of all the available SSO settings, see the <webAppSecurity> element in .

## Configuring RunAs authentication in Liberty

You can delegate authentication to another identity by configuring the RunAs specification for Liberty.

### About this task

By mapping a specified user identity and optional password to a RunAs role, you can delegate the authentication process to a user that has the RunAs role.

**8.5.5.0** You must enable the appSecurity-2.0 and servlet-3.0 Liberty features and have a user registry for your application to configure the RunAs role.

For more information about RunAs authentication, see “RunAs() authentication” on page 984.

To configure RunAs authentication, complete the following steps:

### Procedure

1. **8.5.5.0** Enable the appSecurity-2.0 and servlet-3.0 Liberty features in the server.xml file.
2. Configure a user registry for your application.
3. Specify the <run-as> element in the deployment descriptor of your application.

The following example of web.xml file specifies subsequent calls be delegated to the user that is mapped to the role of Employee:

```
<servlet id="Servlet_1">
  <servlet-name>RunAsServlet</servlet-name>
  <display-name>RunAsServlet</display-name>
  <description>RunAsServlet</description>
  <servlet-class>web.RunAsServlet</servlet-class>
  <run-as>
    <role-name>Employee</role-name>
  </run-as>
</servlet>
```

4. **Distributed operating systems** Map the role that you specified in the previous step to a user. You can do this either in the ibm-application-bnd.xml/xml or in the server.xml file. In the <run-as> element, you must specify a user name. If you are using the ibm-application-bnd.xml file, the password is also required; if you are using the server.xml file, the password is optional. If the password is required, encode the password using the **securityUtility encode** command in the /bin directory. For more information about the **securityUtility** command, see “Liberty:securityUtility command” on page 1844.

The following example uses the <run-as> element within the <application-bnd> element of the server.xml file, where the Employee role has been mapped to the RunAs user of user5:

```
<application-bnd>
  <security-role name="Employee">
    <user name="user1" />
    <user name="user5" />
    <run-as userid="user5" password="{xor}Lz4sLCgwLTs=" />
  </security-role>
</application-bnd>
```

**Note:**

- Because the password is optional in the server.xml file, you can also use the following code for a user without a password:

```
<application-bnd>
  <security-role name="Employee">
    <user name="user1" />
    <user name="user5" />
    <run-as userid="user5" />
  </security-role>
</application-bnd>
```

- If you specify the <application-bnd> element in the server.xml file, your application must not be in the dropins folder. If you leave your application in the dropins folder, then you must disable application monitoring by setting the following in your server.xml file:

```
<applicationMonitor dropinsEnabled="false" />
```

The RunAs user name needs to be unique, and does not exist in external accounts. For example, if you authenticate a user to a SAML identity provider or OpenID Connect provider, make sure the RunAs user name is not in those external accounts.

For more information about the run-as element, see .

5. **z/OS** Configure RunAs authentication via SAF resource profiles, which is specific for z/OS users.

- a. **z/OS** Enable RunAs delegation via SAF.

```
<safAuthorization enableDelegation="true" />
```

- b. **z/OS** Assign the RunAs user identity to the app resource and role. This is done by setting the RunAs user identity into the APPLDATA field of the corresponding SAF resource profile. By default, the corresponding SAF resource profile for a given application and role is named {profilePrefix}.{appName}.{roleName} in the EJBROLE SAF class.

This is the same resource profile used by Liberty SAF Authorization for authorizing users to the application and role. The name of the profile is governed by the safRoleMapper configuration. For more information about mapping application and role names to SAF profile names, see Controlling how roles are mapped to SAF Profiles. Here are some example RACF commands for assigning user5 as the RunAs user for the application myapp and the role of Employee:

```
RDEFINE EJBROLE BBGZDFLT.myapp.Employee UACC(READ)
RALTER EJBROLE BBGZDFLT.myapp.Employee APPLDATA('user5')
SETROPTS GENERIC(EJBROLE) REFRESH
SETROPTS RACLIST(EJBROLE) REFRESH
```

## Configuring TAI in Liberty

You can configure Liberty to integrate with a third-party security service by using Trust Association Interceptors (TAI). The TAI can be called before or after single sign-on (SSO).

### Before you begin

Make sure that you have already installed a third-party security server as a reverse proxy server. The third-party security server can act as a front-end authentication server when the Liberty server applies its own authorization policy onto the resulting credentials, which are passed by the proxy server. You must also have a JAR file that contains the custom TAI class, which implements the com.ibm.wsspi.security.tai.TrustAssociationInterceptor interface.

**Note:** There is no support for monitoring changes of this JAR file.

## About this task

A TAI is used to validate HTTP requests between a third-party security server and a Liberty server. The TAI inspects the HTTP requests from the third-party security server to see whether they contain any security attributes. If the process of validating a request by the TAI is successful, the Liberty server authorizes the request by checking whether the client user has the required permission to access the resources.

For more information of custom TAI and SSO configuration with LTPA, see “Developing a custom TAI for Liberty” on page 1998 and “Customizing SSO configuration using LTPA cookies in Liberty” on page 1887.

You can also use the developer tools to configure a TAI service. **Distributed operating systems** For more information about the tools support, see “Configuring TAI on Liberty by using developer tools” on page 1891.

## Procedure

1. Enable the appSecurity-2.0 Liberty feature in the server.xml file.

```
<featureManager>
  <feature>appSecurity-2.0</feature>
</featureManager>
```
2. Deploy your applications to the Liberty server and enable all Liberty features, such as, jsp-2.2 and jdbc-4.0.
3. Place the TAI implementation library simpleTAI.jar in your server directory.
4. Update the server.xml file with the TAI configuration options and location of the TAI implementation library.

In the following server.xml file, the custom TAI is enabled, but does not do any authentication for unprotected URIs and does not allow to fallback to application authentication method if the TAI authentication fails. As shown in the example, the following configuration elements are available for TAI support:

- trustAssociation
- interceptors
- properties

```
<trustAssociation id="myTrustAssociation" invokeForUnprotectedURI="false"
  failOverToAppAuthType="false">
  <interceptors id="simpleTAI" enabled="true"
    className="com.sample.SimpleTAI"
    invokeBeforeSSO="true" invokeAfterSSO="false" libraryRef="simpleTAI">
    <properties prop1="value1" prop2="value2"/>
  </interceptors>
</trustAssociation>

<library id="simpleTAI">
  <fileset dir="${server.config.dir}" includes="simpleTAI.jar"/>
</library>
...
```

**Note:** The property name cannot start with a period (.), **config.**, or **service**. Also, the property name **id** or **ID** is not allowed.

**Note:** By default, the invokeBeforeSSO property is set to true. By using this setting TAI is invoked even when the SSO token is present and valid. However, if the expected behavior is to invoke TAI

only when the SSO token is invalid or not present, then this property can be disabled by setting it to false, and enabling the `invokeAfterSSO` property. By using this setting TAI is invoked only when the SSO token is not present or is invalid. In some cases, this setup might improve the performance of your system.

For more information about the `<trustAssociation>`, `<interceptors>` and `<properties>` elements, see also .

## Configuring TAI on Liberty by using developer tools

### Distributed operating systems

You can configure a TAI service for Liberty using developer tools.

### Before you begin

For a description of the underlying process of configuring a server, and detailed information about specific aspects of server configuration, see “Administering Liberty manually” on page 1564.

**Avoid trouble:** There are several security configuration examples on the `WASdev.net` website for reference when configuring security for your applications on Liberty.

### Procedure

1. Select the parent **Trust Association Interceptor** and enter an **ID** name.
2. Select the child **Trust Association Interceptor** and configure the **Class name** which is the fully qualified name of your TAI implementation class, then click the arrow next to the **Add** button and select **Global Element** to enter the shared library information.
3. Enter the **ID** for the shared library in the popup window and click **OK**.
4. Configure the **Name** and **Description** fields for the shared library, then click the arrow next to the **Add** button and select **Child Element** to add a fileset reference as a child element.
5. Configure the **Fileset**. Click **Browse** in the **Base directory** field and select the directory where the JAR file is located. Then, click **Browse** in the **Includes pattern** field to select your JAR file that contains your TAI implementation.
6. Configure **Interceptor properties** details by clicking **Add** to add properties for the interceptor.
7. Save the configuration. You can find the following configuration saved in the `server.xml` file.

```
<trustAssociation id="myTrustAssociation" invokeForUnprotectedURI="false"
    failOverToAppAuthType="false">
  <interceptors id="simpleTAI" enabled="true"
    className="com.ibm.websphere.security.sample.SimpleTAI"
    invokeBeforeSSO="true" invokeAfterSSO="false" libraryRef="simpleTAI">
    <properties hostName="machine1" application="test1"/>
  </interceptors>
</trustAssociation>

<library id="simpleTAI">
  <fileset dir="{server.config.dir}" includes="simpleTAI.jar"/>
</library>
```

## Configuring a custom form login page



8.5.5.4

Liberty provides the ability to define a custom form login page for users to submit authentication credentials.

## About this task

You can customize your own custom form login page, but you must implement this page in the required form-based authentication format as specified in the Servlet 3.0 specification. In all forms, the action on the form element must be `j_security_check`. The action must use the `j_username` input field to get the user name and the `j_password` input field to get the user password in forms supporting authentication schemes that require a user name and password. The custom form login page must be provided as an unprotected web resource. You can set this login page at the global server level, which applies to all applications deployed to the server. Alternatively, you can specify the login page for individual applications.

**Note:** Make sure that any files included in your form-login page (such as external style sheets, or images) are unprotected.

## Procedure

1. Specify the following form elements in the form login page that expects a user name and password.

```
<FORM action="j_security_check" method="POST">  
  User name: <INPUT type="text" name="j_username"><br>  
  Password: <INPUT type="password" name="j_password"><br>  
  <INPUT type="submit" name="action" value="Login">  
</FORM>
```

2. Configure the login form for use by applications on the server. There are two possible configurations to use a form login page in an application that is deployed to the server. You can configure the custom login page for use in a single application, or you can configure the page as a global login form that is used for all applications that are deployed to the server.

- a. Configure a login form for a single application. You can configure individual applications to direct users to a specific form login page by configuring the `web.xml` file that is packaged with the application.

Specify the path to the login page in the `web.xml` file that is packaged with the application; for example:

```
<login-config>  
  <auth-method>FORM/<auth-method>  
  <realm-name>MyRealm/<realm-name>  
  <form-login-config id="FormLoginConfig_1">  
    <form-login-page>/login.jsp/<form-login-page>  
    <form-error-page>/loginError.jsp/<form-error-page>  
  </form-login-config>  
</login-config>
```

To see how to customize and package a form login page, refer to [Customizing web application login](#).

- b. Configure a global login form. You can omit the form login page from the `web.xml` files that are packaged with each application and instead, specify in the `server.xml` configuration that the login form is for global use among applications that are deployed to the server.

In the `server.xml` file, include a `webAppSecurity` element with the `loginFormURL` attribute that is specified with a value of the path of the login form page; for example:

```
<webAppSecurity loginFormURL="myGlobalFormLogin/myLogin.jsp" />
```

Ensure that the form login page is packaged as a web application archive (WAR) file deployed to the server.

If the `form-login-page` element within an application's `web.xml` file does not exist, use the global login page that is specified in the server configuration.

3. **Optional:** Configure a custom form login page for OpenID.
4. **Optional:** Configure a custom form login page for OAuth.

## Configuring a custom form login page for OpenID



8.5.5.4

Login pages for Liberty must have a certain configuration in order to support OpenID Authentication.

### About this task



If you have configured the `providerIdentifier` attribute of the `<openid>` element in your `server.xml` file, you can skip this task.

Unlike standard form login pages that require a user name and password, form login for OpenID only requires submitting an OpenID Identifier. You must therefore configure form login pages to accept this OpenID Identifier.

### Procedure

1. Configure the login form to specify `j_security_check` as the value for the action.
2. Add an input field to the login form and set the `name` attribute to `openid_identifier` for users to input an OpenID Identifier. The resulting form is similar to the following HTML example:

```
<FORM action="j_security_check" method="POST">  
  OpenID: <INPUT type="text" name="openid_identifier"><br>  
  <INPUT type="submit" name="action" value="Login">  
</FORM>
```

No user name or password inputs are required if authentication is only performed using OpenID.

## Configuring a custom form login page for OAuth



8.5.5.4

You can configure custom form login pages for specific OAuth service providers.

### About this task

To use a custom form login page for a specific OAuth service provider, you must update the service provider definition in the `server.xml` file.

### Procedure

In the provider configuration, add the `customLoginURL` attribute and specify the login page URL as the value.

The following is an example custom login page entry in the provider definition:

```
<oauthProvider id="OAuthConfigSample"  
  customLoginURL="https://acme.com:9043/oauth20/login.jsp">
```

The login form that is used for OAuth must be configured to accept a user name and password.

## Configuring SAML Web Browser SSO in Liberty



8.5.5.7

You can configure a Liberty server to function as a SAML web browser Single-Sign-On (SSO) service provider.

## About this task

You can configure a Liberty server as a SAML web SSO service provider by enabling the `samlWeb-2.0` feature in Liberty, and in addition to other configuration information.

### Procedure

1. Add the `samlWeb-2.0` Liberty feature to your `server.xml` file by adding the following element declaration inside the `featureManager` element.

```
<feature>samlWeb-2.0</feature>
```

2. Liberty provides a default `samlWebSso20` element.

```
<samlWebSso20 id="defaultSP">
```

```
</samlWebSso20>
```

In this default configuration, the following default values are assumed:

- AssertionConsumerService URL:  
`https://<hostname>:<sslport> /ibm/saml20/defaultSP/acs`
- Service Provider (SP) metadata URL:  
`https://<hostname>:<sslport> /ibm/saml20/defaultSP/samlmetadata`

You can use a browser to download the metadata for this service provider (SP) by using this URL, and provide the URL to the SAML identity provider to establish federation between this SP and Identity Provider (IdP).

- The IdP metadata file must be copied to the `resources/security` directory on the server, and named `idpMetadata.xml`.
- The issuer name for SAML assertion is used as the security realm, and `NameID` is used as the principal to create an authenticated subject from the SAML assertion.
- The SAML `AuthnRequest` is signed with a private key in the default keystore of the server if the attribute `KeyStoreRef` is not specified. If the `keyAlias` is not configured, then `samlsp` is the default key alias. If the `keyAlias` is not configured, and the keystore only contains one private key, the private key is used in the signature.

**Note:** If you create a new service provider instance, and the `defaultSP` is no longer required, then you must explicitly disable the `defaultSP` instance, by adding the following to the `server.xml` file.

```
<samlWebSso20 id="defaultSP" enabled="false">  
</samlWebSso20>
```

**Note:** It is required that you specify a URL safe String that is not null as the `id` for `samlWebSso20`. If the `id` is missing, then the configuration element is omitted, and is not handled as the `defaultSP`.

**Note:** When SAML is configured and enabled, all unauthenticated requests will use SAML authentication. To configure the types of requests that should and should not use SAML authentication, you must configure an authentication filter as described in step 15.

3. Optional: You can add `<samlWebSso20 id="defaultSP">` to the `server.xml` file, and customize the `defaultSP` service provider. For example:
  - `idpMetadata`: Add this parameter to change the IdP metadata location and file name from the default location and file name (`${server.config.dir}/resources/security/idpMetadata.xml`).
  - `userIdentifier`: Add this parameter to select a SAML attribute name whose value is used as the principal name.
  - `groupIdIdentifier`: Add this parameter to select a SAML attribute name whose values are included as group members in the subject.
  - `realmName`: Use this parameter to explicitly specify the realm name to identify a SAML principal in this service provider. The default realm name is the SAML issuer name.

- Optional: You can create one or more new `samlWebSso20` elements with a different ID. For example, if you create a new element with an ID as `mySP`, you effectively create a new SAML SP instance that has a new `AssertionConsumerService` URL:

`https://<hostname>:<sslport>/ibm/saml20/mySP/acs`

**Note:** The ID you choose for `samlWebSso20` is included in URL of the SP, including the `AssertionConsumerService` URL and metadata URL. The `samlWebSso20` ID must be non-empty and must not contain unsafe URL characters.

- Optional: You can configure a trust engine. The Liberty SAML SP supports two types of trust engines:

- **Metadata trust engine:** Validates the signature against information that is provided in the configured IdP metadata.
- **PKIX trust engine:** Validates the trustworthiness of the certificate in the signature through PKIX validation. Certificates that pass this validation are assumed to be trusted.

Metadata is the default trust engine. If you want to use the PKIX trust engine, you need to add the `PKIXTrustEngine` element, and define the proper `trustAnchor`.

- Optional: You can configure how to create an authenticated subject from SAML. By default the Liberty SP creates a subject from SAML assertion directly without the requirement of a local user registry, which is equivalent to the configuration `mapToUserRegistry=No`. The other configuration options are `mapToUserRegistry=User` or `mapToUserRegistry=Group`.

- `mapToUserRegistry=No`: The SAML issuer's name is `realm`, and the `NameID` is used to create a principal name and unique security name in the subject, and no group member is included. You can configure the attributes: `userIdentifier`, `realmIdentifier`, `groupIdentifier`, and `userUniqueIdentifier` to create an authenticated subject with a customized user name, realm name, group memberships, and unique security identifier.
- `mapToUserRegistry=User`: Choose this option if you want to validate a SAML user against your on-premises user registry, and create the user subject based on the on-premises registry.
- `mapToUserRegistry=Group`: Choose this option if you want to validate a SAML group against your local user registry, and create a subject to contain those validated groups. This option is similar to `mapToUserRegistry=No`, except for group memberships are verified against the on-premises user registry.

- Optional: You can implement the Liberty SAML SPI, `com.ibm.wsspi.security.saml2.UserCredentialResolver` as a user feature to dynamically map a SAML assertion to a Liberty subject.
- Optional: You can define rules to tell the IdP how to authenticate a user by configuring one or more of the following attributes when using an SP-initiated Web SSO flow: `forceAuthn`, `isPassive`, `allowCreate`, `authnContextClassRef`, and `authnContextComparisonType`.
- Optional: You can define a required `NameID` format in the `AuthnRequest` by using the `nameIDFormat` attribute. You can specify any `NameID` format that is defined in the SAML specification, or use the keyword `customize` to specify the custom `NameID` format.
- Optional: You can configure multiple SP and IdP federation partners by creating multiple `samlWebSso20` elements, and each `samlWebSso20` refers to one unique `authFilter` element. All `authFilters` must exclude each other. With multiple `samlWebSso20` configured, each can perform single-sign-on with its federated identity provider, and has its own authentication policy and consuming rules.
- Optional: Add support for IdP-initiated unsolicited SSO. Liberty SAML SP supports IdP-initiated unsolicited SSO with and without the requirement of IdP metadata on-premises. If you do not have IdP metadata, or if you intend to use unsolicited SSO to federate with multiple identity providers with one Liberty SP, you must add the following configurations:
  - Configure `<PKIXTrustEngine>`, and import all the IdP signer certificates to the default truststore of the Liberty server, or to the `trustAnchor` of the `PKIXTrustEngine`.

- Configure the trustedIssuers to list the issuer name of the IdP as it appears in the SAML assertion. The issuer name is used as the EntityID in the metadata.
  - If you intend to support unsolicited SSO only, you can configure SP-initiated unsolicited SSO as documented in the next step. This scenario is useful if the user's security context in the SP that is associated with SAML becomes invalid, the SP can redirect the user back to the IdP to start unsolicited SSO again automatically.
12. Optional: Add support for SP-initiated unsolicited SSO. The Liberty SAML SP uses configured IdP metadata to perform a solicited SAML AuthnRequest. It is possible for the Liberty SP to redirect unauthenticated requests to a preconfigured login application without using AuthnRequest. This scenario is useful if a business application performs pre-authentication processing before a user can authenticate to the SAML IdP, or the SAML IdP must be hidden from the Liberty SP. To configure this scenario, you add the loginPageURL attribute, and set its value to a URL that can instruct a user to authenticate to the SAML IdP.
  13. Optional: Configure signature requirements with the following considerations:
    - SAML assertion. All SAML assertions must be digitally signed by the SAML IdP. In the rare case that you want to accept an unsigned assertion, you can explicitly configure wantAssertionsSigned=false.
    - The default signature algorithm is SHA256. If you must change the algorithm, use the signatureMethodAlgorithm attribute to modify it.
    - If you do not want to sign the SAML AuthnRequest, you can set authnRequestsSigned=false.
  14. Optional: You can configure an SP authentication session and cookie. After SAML assertion is verified and processed, the Liberty SAML SP maintains an authenticated session between the browser and the SP without using an LTPA cookie. The authenticated session timeout is set to SessionNotOnOrAfter in the <saml:AuthnStatement> if presented, or to sessionNotOnOrAfter as configured in the server.xml file, with the default being 120 minutes. The session cookie name is automatically generated, and you can customize the cookie name by using the attribute spCookieName to specify the wanted name.

If you want the Liberty SP to create an LTPA cookie from the SAML assertion and use the LTPA cookie for subsequent authentication requests, you can add the configuration disableLtpaCookie=false. If you want to share the LTPA cookie with other servers, you must add the configuration attribute allowCustomCacheKey="false".

**Note:** If you configure disableLtpaCookie="false" and allowCustomCacheKey="false", ensure that a SAML user name is not directly authenticating to an on-premises user registry that prevents a user from having two accounts.

15. Optional: Configure the Authentication Filter.
 

When the samlWeb-2.0 feature is enabled, any unauthenticated request is authenticated through one SAML SP. If you define a customized samlWebSso20 element, all authentication requests are handled by this samlWebSso20 SP instance; otherwise, all authentication is handled by the default instance defaultSP. You can use authnFilter to define which SP instance to handle the authentication request.

For more information on configuring the authentication filter, see Authentication Filters.
16. Optional: Configure the SAML SP in a cluster.
 

If application servers are cluster members, and you use a router or reverse proxy server to route your requests, then you need to perform the following tasks:

  - The router and proxy server must be configured to support session affinity.
  - Add the configuration attribute spHostAndPort to each application server, and set its value to the router or proxy server host name and port. For example, spHostAndPort="https://myRouter.com:443".
  - Generate an X509 certificate for signing the SAML AuthnRequest, and use this certificate on all application servers. For example, you can create a keystore to contain this certificate only, and add the KeyStoreRef to reference this keystore on all application servers.

- If `createSession="true"` is not set in a cluster environment, then the following error is encountered during the stress execution:

E CWWKS5029E: The relay state [sp\_initial\_KGe22fCWKG11D9VkoMuDz0Ji8pBxFPnU] in the response from the identity pro

Here is a sample cluster configuration:

```
<keyStore id="samlKeyStore" password="<password>"
  location="{server.config.dir}/resources/security/<samlKey.jks>" />

  <samlWebSso20 id="defaultSP"
    spHostAndPort="https://<IHS host>:<port>"
    keyStoreRef="samlKeyStore"
    createSession="true"
    allowCustomCacheKey="false"
    disableLtpaCookie="false"
    mapToUserRegistry="User">
</samlWebSso20>
```

## Results

You have now established the configuration that is required to configure a Liberty server as a SAML service provider capable of single-signing on with SAML identity providers.

## Using OpenID Connect



8.5.5.4

OpenID Connect in the Liberty server is implemented as an OAuth 2.0 extension. In addition to providing OpenID Connect functions, the OpenID Connect provider supports all OAuth 2.0 functions.

### OpenID Connect endpoint URLs



8.5.5.4

Learn about OpenID Connect endpoint URLs that are available for communicating with the OpenID Connect provider.

After OpenID Connect is configured, several endpoint URLs are available on Liberty so that OpenID Connect clients can communicate with the OpenID Connect provider before accessing protected resources. By default, all communications must be over Transport Layer Security (TLS).

The following endpoint URLs are available for communicating with the OpenID Connect provider:

- “Authorization endpoint URL”
- “Token endpoint URL” on page 1898
- “Introspection endpoint URL” on page 1898
- “UserInfo endpoint URL” on page 1898
- “Discovery endpoint URL” on page 1898
- “Coverage map endpoint URL” on page 1899
- “Registration endpoint URL” on page 1899

### Authorization endpoint URL

`https://<host_name>:<port_number>/oidc/endpoint/<provider_name>/authorize`

where

#### **host\_name**

The host name of the OpenID Connect provider.

#### **port\_number**

The secure port number that is configured on the Liberty server.

**provider\_name**

The OpenID Connect provider name.

For more information, see  [8.5.5.4](#) Invoking the Authorization Endpoint for OpenID Connect.

**Token endpoint URL**

`https://<host_name>:<port_number>/oidc/endpoint/<provider_name>/token`

where

**host\_name**

The host name of the OpenID Connect provider.

**port\_number**

The secure port number that is configured on the Liberty server.

**provider\_name**

The OpenID Connect provider name.

For more information, see  [8.5.5.4](#) Invoking the Token Endpoint for OpenID Connect.

**Introspection endpoint URL**

`https://<host_name>:<port_number>/oidc/endpoint/<provider_name>/introspect`

where

**host\_name**

The host name of the OpenID Connect provider.

**port\_number**

The secure port number that is configured on the Liberty server.

**provider\_name**

The OpenID Connect provider name.

For more information, see  [8.5.5.4](#) Invoking the Introspection Endpoint for OpenID Connect.

**UserInfo endpoint URL**

`https://<host_name>:<port_number>/oidc/endpoint/<provider_name>/userinfo`

where

**host\_name**

The host name of the OpenID Connect provider.

**port\_number**

The secure port number that is configured on the Liberty server.

**provider\_name**

The OpenID Connect provider name.

For more information, see  [8.5.5.4](#) Invoking the UserInfo Endpoint for OpenID Connect.

**Discovery endpoint URL**

`https://<host_name>:<port_number>/oidc/endpoint/<provider_name>/.well-known/openid-configuration`

where

**host\_name**

The host name of the OpenID Connect provider.

**port\_number**

The secure port number that is configured on the Liberty server.

**provider\_name**

The OpenID Connect provider name.

For more information, see  [8.5.5.4](#) Configuring an OpenID Connect Provider to accept discovery requests.

**Coverage map endpoint URL**

`https://<host_name>:<port_number>/oidc/endpoint/<provider_name>/coverage_map`

where

**host\_name**

The host name of the OpenID Connect provider.

**port\_number**

The secure port number that is configured on the Liberty server.

**provider\_name**

The OpenID Connect provider name.

For more information, see  [8.5.5.4](#) Invoking the coverage map service.

**Registration endpoint URL**

`https://<host_name>:<port_number>/oidc/endpoint/<provider_name>/registration`

where

**host\_name**

The host name of the OpenID Connect provider.

**port\_number**

The secure port number that is configured on the Liberty server.

**provider\_name**

The OpenID Connect provider name.

For more information, see  [8.5.5.4](#) Configuring an OpenID Connect Provider to accept client registration requests.

**Configuring an OpenID Connect Provider in Liberty**

[8.5.5.4](#)

You can configure a Liberty server to function as an OpenID Connect Provider, or authorization server, to take advantage of web single sign-on.

**About this task**

You can configure a Liberty server to act as an OpenID Connect Provider by enabling the `openidConnectServer-1.0` feature in Liberty, and in addition to other configuration information.

## Procedure

1. Add the openidConnectServer-1.0 Liberty feature and any other needed features to the server.xml file. The ssl-1.0 feature is also required for the openidConnectServer-1.0 feature.

```
<feature>openidConnectServer-1.0</feature>
<feature>ssl-1.0</feature>
```

2. Define an OAuth service provider. OpenID Connect is built on top of the OAuth 2.0 protocol and you must configure a valid OAuth service provider. The configuration of an OAuth service provider includes the appropriate oauth-roles, oauthProvider, and user registry elements. Any user that is authorized to use OpenID Connect must also be mapped to the authenticated oauth-role. See Defining an OAuth service provider for more information.

The OAuth metadata is updated for OpenID Connect, and the main additions are in the client metadata. If you use the databaseStore mode for client registration, see “Configuring an OpenID Connect Provider to accept client registration requests” on page 1915 for more information. It is suggested that you follow the document to manage clients. If you use the localStore mode for client registration, you can register the scope, preAuthorizedScope, grantTypes, responseTypes, introspectTokens, and functionalUserId, as well as other attributes.

3. Add an openidConnectProvider element whose oauthProviderRef attribute references the configured oauthProvider. Each oauthProvider can only be referenced by one openidConnectProvider, and two or more openidConnectProvider elements cannot reference to the same oauthProvider. The name attribute and the secret attribute of the client element must match the client ID and the client secret of the corresponding OpenID Connect Client. This example works with the default Liberty server OpenID Connect Client.

**Note:** In this example, the OP expects the client's SSL port to be set to 443.

```
<openidConnectProvider id="OidcConfigSample" oauthProviderRef="OAuthConfigSample" />

<oauthProvider id="OAuthConfigSample">
<localStore>
<client name="client01" secret="{xor}LDo8LTor"
displayname="client01"
scope="openid profile email"
redirect="https://server.example.com:443/oidcclient/redirect/client01"/>
</localStore>
</oauthProvider>
```

**Note:** A valid client must register its name, redirect, scope, and secret for authorization\_code grant type.

4. Configure the truststore of the server to include the signer certificates of the OpenID Connect Relying Parties, or clients, that are supported. For information about keystores, see “Enabling SSL communication in Liberty” on page 1834
5. Modify the SSL configuration of the server to use the configured truststore.

```
<sslDefault sslRef="DefaultSSLSettings" />
<ssl id="DefaultSSLSettings" keyStoreRef="myKeyStore" trustStoreRef="myTrustStore" />
<keyStore id="myKeyStore" password="{xor}Lz4sLCgwLTs=" type="jks" location="{server.config.dir}/resources/security/Bas
<keyStore id="myTrustStore" password="{xor}Lz4sLCgwLTs=" type="jks" location="{server.config.dir}/resources/security/B
```

OpenID Connect is configured to use the default SSL configuration that is specified by the server. Therefore, the default SSL configuration for the server must use the truststore that is configured for OpenID Connect.

The user consent form in OpenID Connect is pluggable, which allows providers to create and maintain their own consent form. Because this form is retrieved over SSL, you must configure the truststore to include the signer certificate of the server on which the consent form is hosted. If the default consent form is used and the truststore that is used for OpenID Connect is configured to be different from the keystore that is used by the Liberty server, you must import the Liberty server's signer certificate into the OpenID Connect truststore.

For more OpenID Connect Provider configuration options, see .

**Note:** In order to use OpenID Connect, the scope attribute must include openid in the scope list.

## Results

You have now completed the minimum configuration that is required to configure a Liberty server as an OpenID Connect Provider capable of communicating with other Liberty servers configured as OpenID Connect Clients.

### Using an OpenID Connect provider as an OAuth 2.0 authorization server: 8.5.5.4

An OpenID Connect provider can be used as a normal OAuth 2.0 authorization provider to issue an OAuth 2.0 access\_token, and support all OAuth 2.0 grant types.

An OpenID Connect provider supports JSON Web Token (JWT) Bearer Token as a grant for requesting an OAuth 2.0 access token, see  JSON Web Token (JWT) for OAuth Client Authorization Grants and  Configuring an OpenID Connect Provider to accept JSON Web Tokens (JWT) for authorization grants.

If an authorization request is made with an authorization code grant or implicit grant type, and if openid scope is not included or approved, the request is handled as a normal OAuth authorization request. An id\_token is not issued, and an access\_token and refresh\_token can be issued.

An OpenID Connect provider can support OAuth authorization flow with Resource Owner Password Credentials Grant or Client Credentials Grant, see  Configuring an OpenID Connect Provider to enable 2-legged OAuth requests.

### JSON Web Token (JWT) for OAuth Client Authorization Grants: 8.5.5.4

JWT for OAuth Client Authorization Grants enables a client to send a signed JWT token to the OpenID Connect Provider in exchange for an OAuth 2.0 access token.

JWT for OAuth Client Authorization Grants is included in the openidConnectServer-1.0 feature. It enables a client to send a signed JWT token to the OpenID Connect Provider in exchange for an OAuth 2.0 access token.

An example usage scenario of this functionality might be a customer of an electric company who authorizes automatic monthly payments from an online bank. Assuming the electric company and the online bank have established a trusted relationship for the purposes of fulfilling such requests. The electric company can send a signed JWT Token with proper claims to the token endpoint URI of the OpenID Connect Provider that are configured for the online bank in order to request an OAuth 2.0 access token each month. The electric company can then use the access token to cash monthly payments from the online bank.

Portions of the JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants specification are supported for Liberty servers that are configured as OpenID Connect Providers. Users that want to support the JWT client functionality must do so by using their own application.

- Authorized scopes
- Claims in a JSON Web Token
- Submitting JSON Web Token requests

## Authorized scopes

The OpenID Connect Client sends an HTTPS request with a JWT to the token endpoint of the OpenID Connect Provider to request an access token. During this process, the user sees no consent form for authorizing the use of scopes. The JWT handler will handle the authorized scopes that are based on the following criteria:

1. If no scope parameter is specified in the request, the OpenID Connect Provider will not specify any scopes in the access token.
2. When an OpenID Connect Client is qualified as an autoAuthorized client in the OpenID Connect Provider configuration, any scope that is specified by the client in the request is specified in the scope list of the access token.
3. When an OpenID Connect Client is not qualified as an autoAuthorized client, the scope that is included in the request needs to be filtered by the list of scopes in the client configuration and must also be specified in the preAuthorizedScope list. If a scope in the HTTPS request is in the scope and preAuthorizeScope list of the client configuration, the scope can be specified in the scope list of the access token.

When a client is not qualified as an autoAuthorized client, scopes that can be included in the scope list of the access token must be properly configured in the client configuration. The scope must be included in the values for the scope and preAuthorizedScope attributes in the client configuration for the OpenID Connect Provider. In the example that is shown, the scopes profile and email are specified in the scope list of the access token because both are included in the scope and preAuthorizedScope value list. If a scope is not listed in the scope attribute of the client configuration, it is omitted from the scope list of the access token. If a scope is listed in the scope attribute but is not included in the preAuthorizedScope list within the client configuration, the authorization request triggers an invalid\_grant error in the response from the OpenID Connect Provider.

```
<openidConnectProvider id="OidcConfigSample" oauthProviderRef="OAuthConfigSample" />
<oauthProvider id="OAuthConfigSample" ... >
  ...
  <localStore>
    <client name="client01" secret="{xor}..."
      displayname="client01"
      scope="profile email phone"
      preAuthorizedScope="profile email"
      enabled="true"/>
    ...
  </localStore>
</oauthProvider>
```

## Claims in a JSON Web Token

A valid JSON Web Token must be signed. A Liberty server that is configured as an OpenID Connect Provider only supports HMAC-SHA256 as the token signing algorithm. The signing key for each OpenID Connect Client is the secret attribute in the client configuration of the OpenID Connect Provider. In the example that is shown, the signing key that is used would be "{xor}LDo8LTor".

```
<client name="client01" displayname="client01" secret="{xor}LDo8LTor" ... />
```

The OpenID Connect Provider also verifies the following claims in a JWT:

### 'iss' (issuer)

This claim is required in a JWT. The iss claim must match the name attribute or the redirect attribute of the client configuration in the OpenID Connect Provider. In the following example, the iss claim must match either client01 or http://op201406.ibm.com:8010/oauthclient/redirect.jsp.

```
<client name="client01" redirect="http://op201406.ibm.com:8010/oauthclient/redirect.jsp" scope="openid profile email" />
```

**'sub' (subject)**

This claim is required in a JWT. The value of the subject must be a valid user name in the user registry of the OpenID Connect Provider server.

**'aud' (audience)**

This claim is required in a JWT. The value of the audience claim is the name of the issuerIdentifier when the issuerIdentifier attribute is specified in the openidConnectProvider configuration. If the issuerIdentifier attribute is not specified in the openidConnectProvider configuration, the audience must be the token endpoint URI of the OpenID Connect Provider. In the following example, the value of the audience claim would be "OpenIDConnectProviderID1".

```
<openidConnectProvider id="OidcConfigSample" oauthProviderRef="OAuthConfigSample" issuerIdentifier="OpenIDConnectProviderID1">
```

**'exp' (expiration)**

This claim is required in a JWT and limits the time window that the JWT can be used. The OpenID Connect Provider verifies the exp against its system clock, plus some allowable clock skew.

**'nbf' (not before)**

This is an optional claim. When present, the token is only valid after the time specified by this claim. The OpenID Connect Provider verifies this time against its system clock, plus some allowable clock skew.

**'iat' (issued at)**

By default, this is an optional claim. However, if the iatRequired attribute of the jwtGrantType element is set to true, then all JWTs are required to contain the iat claim. When present, the iat claim indicates the time at which the JWT was issued. A JWT cannot be issued longer than the maxTokenLifetime.

**'jti' (JWT ID)**

This is an optional claim and is the unique identifier of a JWT Token. When present, the same JWT ID cannot be reused by an issuer. For example, if client01 issues a JWT whose jti is id6098364921, then no other JWT issued by client01 can have a jti value of id6098364921. A JWT with a jti claim identical to another JWT is considered to be a replay attack. Liberty servers that are configured as OpenID Connect Providers set up a jti cache on the server. The size of the cache is specified by the maxJtiCacheSize in the jwtGrantType configuration. The jti IDs that are kept in the cache are checked against any new incoming jti ID. The jti IDs stored in the cache are not discarded unless the cache is full.

**Submitting JSON Web Token requests**

It is a best practice to use the HTTPS protocol instead of HTTP to submit a JWT request. The token endpoint of the OpenID Connect Provider is used for handling HTTPS JWT requests. To determine the token endpoint for the OpenID Connect Provider, see Invoking the Token Endpoint for OpenID Connect or OAuth endpoint URLs.

The request must contain the following parameters:

- grant\_type - The value of this parameter must be "urn:ietf:params:oauth:grant-type:jwt-bearer"
- assertion - The value of this parameter must contain a single signed JWT Token.
- scope - This parameter is optional. If scope is omitted, the access token that is returned does not contain any scopes. The scope values listed in the scope parameter are checked against the OpenID Connect Provider configuration. For more information, see the previous Authorized Scopes section.
- client\_id - The value of this parameter must match the name attribute in the client configuration of the OpenID Connect Provider.
- client\_secret - The value of this parameter must match the secret attribute in the client configuration of the OpenID Connect Provider.

An example HTTPS request:

```

POST /token.oauth2 HTTP/1.1
Host: oidc.ibm.com
Content-Type: application/x-www-form-urlencoded

client_id=client01
&client_secret=secret
&grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-bearer
&assertion=eyJhbGciOiJIcGkiLCJ0eSI6ImF4fQ.MB6ZF1CsHg5MJ-weiHZYz6xgF1jdSZn7ErchHs8-8Rk
&scope=profile email

```

A Java example to create a signed JWT Token:

```

package com.ibm.sample;

import java.security.SignatureException;
import com.google.gson.JsonObject;
import net.oauth.jsontoken.crypto.HmacSHA256Signer;

import net.oauth.jsontoken.SystemClock;
import net.oauth.jsontoken.JsonToken;
import org.joda.time.Duration;
import org.joda.time.Instant;

public class SampleJWTToken {
    private static final Duration SKEW = Duration.standardMinutes(5);

    JsonToken jwtToken = null;
    String[] allPayloadKeys = { "iss", "sub", "aud", "exp", // required
                               "nbf", "iat", "jti" }; // optional

    public SampleJWTToken(String clientId,
                          String keyId,
                          String signKey,
                          String audience,
                          String subject, // user
                          String jtiId) throws Exception { // InvalidKeyException

        byte[] hs256Key = signKey.getBytes();
        HmacSHA256Signer hmacSha256Signer = new HmacSHA256Signer(
            clientId, keyId, hs256Key);
        // _rsaSha256Signer = new RsaSHA256Signer(clientId, _keyId,
        //   _privateKey);
        SystemClock clock = new SystemClock(SKEW);
        jwtToken = new JsonToken(hmacSha256Signer, clock);
        JsonObject headerObj = jwtToken.getHeader();
        JsonObject payloadObj = jwtToken.getPayloadAsJsonObject();

        headerObj.addProperty("alg", "HS256");

        Instant instantExp = clock.now().plus(600000); // 10 minutes
        jwtToken.setExpiration(instantExp);
        jwtToken.setAudience(audience);
        payloadObj.addProperty("iss", clientId);
        payloadObj.addProperty("sub", subject);

        // optional
        payloadObj.addProperty("jti", jtiId);
        jwtToken.setIssuedAt(clock.now()); // issued at time
    }

    public String getJWTTokenString() throws Exception {
        String signedAndSerializedString = null;
        try {
            signedAndSerializedString = jwtToken.serializeAndSign();
        } catch (SignatureException e) {
            throw e;
        }
    }
}

```

```

    }
    return signedAndSerializedString;
}
}

```

## Configuring an OpenID Connect Provider to accept discovery requests: 8.5.5.4

The discovery configuration endpoint makes information available about the capabilities that are supported by the OpenID Connect Provider (OP) server.

### About this task

The metadata that is returned by this service is based on and extends the OIDC Discovery 1.0 specification provider metadata. The service returns a set of default configurations if nothing is specified. Otherwise, refer to the list of properties to understand their purpose and possible configurable options.

### Procedure

You can override the default values for selected properties in the discovery configuration service. This action is performed by specifying the values in the `server.xml` file. Refer to the following table of properties to view the configurable properties and possible configuration options.

*Table 130. Discovery request parameters*

Attribute Name	Data Type	Required/Optional	Description
responseTypesSupported	Input	Optional	The response types that are supported by the OpenID Connect Provider (OP) server. Unless specified, the default values are code, token, and id_token token. More than 1 value can be specified. These values are strings. For example, possible values are: <ul style="list-style-type: none"> <li>code</li> <li>token</li> <li>id_token token</li> </ul>
subjectTypesSupported	Output only	N/A	The subject types that are supported by the OP server. This value is set to public. This value is a string.

Table 130. Discovery request parameters (continued)

Attribute Name	Data Type	Required/Optional	Description
idTokenSigningAlgValuesSupported	Output only	Optional	<p>The ID token signing algorithms that are supported by the OP server. This value is specified as the server attribute <code>signatureAlgorithm</code> in the <code>openidConnectProvider</code> server configuration. Unless specified, the default value is HS256. Only 1 value can be specified. This is a string. For example, possible values for attribute <code>signatureAlgorithm</code> in the <code>openidConnectProvider</code> configuration:</p> <ul style="list-style-type: none"> <li>• none</li> <li>• RS256</li> <li>• HS256</li> </ul>
scopesSupported	Input	Optional	<p>The scope values supported by the OP server. Unless specified, the default values are <code>openid</code>, <code>general</code>, <code>profile</code>, <code>email</code>, <code>address</code>, and <code>phone</code>. More than 1 value can be specified. These values are strings. For example, possible values are:</p> <ul style="list-style-type: none"> <li>• <code>openid</code></li> <li>• <code>general</code></li> <li>• <code>profile</code></li> <li>• <code>email</code></li> <li>• <code>address</code></li> <li>• <code>phone</code></li> </ul>

Table 130. Discovery request parameters (continued)

Attribute Name	Data Type	Required/Optional	Description
claimsSupported	Input	Optional	<p>The claims values that are supported by the OP server. Unless specified, the default values are sub, groupIds, name, preferred_username, picture, locale, email, and profile. More than 1 value can be specified. These values are strings. For example, possible values are:</p> <ul style="list-style-type: none"> <li>• sub</li> <li>• groupIds</li> <li>• name</li> <li>• preferred_username</li> <li>• picture</li> <li>• locale</li> <li>• email</li> <li>• profile</li> </ul>
responseModesSupported	Input	Optional	<p>The response modes that are supported by the OP server. Unless specified, the default values are query and fragment. More than 1 value can be specified. These values are strings.</p> <ul style="list-style-type: none"> <li>• query</li> <li>• fragment</li> </ul>
grantTypesSupported	Input	Optional	<p>The grant types that are supported by the OP server. Unless specified, the default values are authorization_code, implicit, refresh_token, client_credentials, password, and urn:iETF:params:oauth:grant-type:jwtbearer. More than 1 value can be specified. These values are strings. For example, possible values are:</p> <ul style="list-style-type: none"> <li>• authorization_code</li> <li>• implicit</li> <li>• refresh_token</li> <li>• client_credentials</li> <li>• password</li> <li>• urn:iETF:params:oauth:grant-type:jwtbearer</li> </ul>

Table 130. Discovery request parameters (continued)

Attribute Name	Data Type	Required/Optional	Description
tokenEndpointAuthMethodsSupported	Input	Optional	The token endpoint authorization methods that are supported by the OP server. Unless specified, the default values are <code>client_secret_post</code> , and <code>client_secret_basic</code> . More than 1 value can be specified. These values are strings. For example, possible values are: <ul style="list-style-type: none"> <li>• none</li> <li>• <code>client_secret_post</code></li> <li>• <code>client_secret_basic</code></li> </ul>
displayValuesSupported	Output only	N/A	The display values supported by the OP server. This value is set to page. This value is a string.
claimTypesSupported	Output only	N/A	The claim type values that are supported by the OP server. This value is set to normal. This value is a string.
claimsParameterSupported	Input	Optional	Indication of whether claims parameter is supported by the OP server. Unless specified, the default value is false. Only 1 value can be specified. This is a Boolean value. For example, possible values are: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>
requestParameterSupported	Input	Optional	Indication of whether a request parameter is supported by the OP server. Unless specified, the default value is false. Only 1 value can be specified. This is a Boolean value. For example, possible values are: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>

Table 130. Discovery request parameters (continued)

Attribute Name	Data Type	Required/Optional	Description
requestUriParameterSupported	Input	Optional	Indication of whether request URI parameter is supported by the OP server. Unless specified, the default value is false. Only 1 value can be specified. This is a Boolean value. For example, possible values are: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>
requireRequestUriRegistration	Input	Optional	Indication of whether require request URI registration is supported by the OP server. Unless specified, the default value is false. Only 1 value can be specified. This is a Boolean value. For example, possible values are: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>

### Examples of discovery configuration

The following example assumes that the Liberty OP is configured with SSL on port 443.

`https://server.example.com:443/oidc/endpoint/<provider_name>/`

The discovery configuration endpoint is accessible at:

`https://server.example.com:443/oidc/endpoint/<provider_name>/.well-known/openid-configuration`

For example, in the `server.xml` file, a user can customize their OpenID Connect discovery configuration properties in the following manner:

```
<openidConnectProvider id="OidcConfigSample" oauthProviderRef="OAuthConfigSample">
  <discovery
    responseTypeSupported="token, id_token token"
    subjectTypesSupported="public"
    scopesSupported="openid, general, profile"
    claimsSupported="sub, groupIds, name"
    responseModesSupported="query"
    grantTypesSupported="implicit"
    tokenEndpointAuthMethodsSupported="client_secret_basic"
    displayValuesSupported="page"
    claimTypesSupported="normal"
    claimsParameterSupported="true"
    requestParameterSupported="true"
    requestUriParameterSupported="true"
    requireRequestUriRegistration="true"
  />
</openidConnectProvider>
<oauthProvider id="OAuthConfigSample">
</oauthProvider>
```

## Example of customized discovery configuration

Request Headers:

GET https://server.example.com:443/oidc/endpoint/<provider\_name>/.well-known/openid-configuration

Response Headers:

Status: 200

Content-Type: application/json

Cache-Control: public, max-age=3600

Response Body:

```
{
  "introspection_endpoint": "https://server.example.com:443/oidc/endpoint/<provider_name>/introspect",
  "coverage_map_endpoint": "https://server.example.com:443/oidc/endpoint/<provider_name>/coverage_map",
  "issuer": "https://server.example.com:443/oidc/endpoint/<provider_name>",
  "authorization_endpoint": "https://server.example.com:443/oidc/endpoint/<provider_name>/authorize",
  "token_endpoint": "https://server.example.com:443/oidc/endpoint/<provider_name>/token",
  "response_types_supported": [
    "token",
    "id_token token"
  ],
  "subject_types_supported": [
    "public"
  ],
  "userinfo_endpoint": "https://server.example.com:443/oidc/endpoint/<provider_name>/userinfo",
  "registration_endpoint": "https://server.example.com:443/oidc/endpoint/<provider_name>/registration",
  "scopes_supported": [
    "openid",
    "general",
    "profile"
  ],
  "claims_supported": [
    "sub",
    "groupIds",
    "name"
  ],
  "response_modes_supported": [
    "query"
  ],
  "grant_types_supported": [
    "implicit"
  ],
  "token_endpoint_auth_methods_supported": [
    "client_secret_basic"
  ],
  "display_values_supported": [
    "page"
  ],
  "claim_types_supported": [
    "normal"
  ],
  "claims_parameter_supported": true,
  "request_parameter_supported": true,
  "request_uri_parameter_supported": true,
  "require_request_uri_registration": true,
  "check_session_iframe": "https://server.example.com:443/oidc/endpoint/<provider_name>/check_session_iframe",
  "end_session_endpoint": "https://server.example.com:443/oidc/endpoint/<provider_name>/end_session"
}
```

## Example of default discovery configuration

Request Headers:

GET https://server.example.com:443/oidc/endpoint/<provider\_name>/.well-known/openid-configuration

Response Headers:

Status: 200

Content-Type: application/json

Cache-Control:public, max-age=3600

Response Body:

```
{
  "introspection_endpoint":"https://server.example.com:443/oidc/endpoint/<provider_name>/introspect",
  "coverage_map_endpoint":"https://server.example.com:443/oidc/endpoint/<provider_name>/coverage_map",
  "issuer":"https://server.example.com:443/oidc/endpoint/<provider_name>",
  "authorization_endpoint":"https://server.example.com:443/oidc/endpoint/<provider_name>/authorize",
  "token_endpoint":"https://server.example.com:443/oidc/endpoint/<provider_name>/token",
  "response_types_supported":[
    "code",
    "token",
    "id_token token"
  ],
  "subject_types_supported":[
    "public"
  ],
  "userinfo_endpoint":"https://server.example.com:443/oidc/endpoint/<provider_name>/userinfo",
  "registration_endpoint":"https://server.example.com:443/oidc/endpoint/<provider_name>/registration",
  "scopes_supported":[
    "openid",
    "general",
    "profile",
    "email",
    "address",
    "phone"
  ],
  "claims_supported":[
    "sub",
    "groupIds",
    "name",
    "preferred_username",
    "picture",
    "locale",
    "email",
    "profile"
  ],
  "response_modes_supported":[
    "query",
    "fragment"
  ],
  "grant_types_supported":[
    "authorization_code",
    "implicit",
    "refresh_token",
    "client_credentials",
    "password",
    "urn:iETF:params:oauth:grant-type:jwt-bearer"
  ],
  "token_endpoint_auth_methods_supported":[
    "client_secret_post",
    "client_secret_basic"
  ],
  "display_values_supported":[
    "page"
  ],
  "claim_types_supported":[
    "normal"
  ],
  "claims_parameter_supported":false,
  "request_parameter_supported":false,
  "request_uri_parameter_supported":false,
  "require_request_uri_registration":false,
  "check_session_iframe":"https://server.example.com:443/oidc/endpoint/<provider_name>/check_session_iframe",
  "end_session_endpoint":"https://server.example.com:443/oidc/endpoint/<provider_name>/end_session"
}
```

## Configuring claims returned by the UserInfo endpoint: 8.5.5.4

You can configure a Liberty OpenID Connect Provider to customize the claims that are returned by the UserInfo endpoint.

### About this task

You can configure the claims that are returned from a Liberty server OpenID Connect Provider by using the `scopeToClaimMap` and `claimToUserRegistryMap` subelements of the `openidConnectProvider` element in the `server.xml` file.

The OpenID Connect UserInfo endpoint accepts an access token as input and returns a set of claims about the user for whom the access token was created. The claims that are returned are determined by:

1. The scopes in the access token  
An access token can have multiple scopes. The scopes in an access token are the scopes that are supplied on the authorization endpoint invocation that created the access token.
2. The claims that are associated with the scopes  
Each scope can have multiple claims that are associated with it.
3. The federated repository properties that are associated with the claims  
A claim can have only one federated repository property that is associated with it.
4. The user registry attributes that are associated with the federated repository properties  
A federated repository property can have only one user registry attribute that is associated with it.

**Note:** The only user registry type that supports the retrieval of UserInfo claims is LDAP.

Liberty defines default scopes, claims, federated registry properties, and default mappings.

*Table 131. Default mappings for scopes, claims, and federated registry properties*

Scope	Claims	Federated registry property
profile	name, given_name, picture	displayName, givenName, photoURL
email	email	mail
address	address	postalAddress
phone	phone_number	telephoneNumber

Each of the following steps is optional. The Liberty server defines default scopes, claims, federated registry properties, and default mappings. The only time that you need to perform any of the following steps is if you want to change a default mapping or define a custom scope or claim.

### Procedure

1. Configure the claims that are associated with scopes. A scope can be mapped to multiple claims, and multiple claims must be comma-separated.

In the following example, the scope `CUSTOM_SCOPE1` is associated with two claims, `CUSTOM_CLAIM1` and `language`, and the scope `CUSTOM_SCOPE2` is associated with the claim `CUSTOM_CLAIM2`.

```
<scopeToClaimMap CUSTOM_SCOPE1="CUSTOM_CLAIM1, language"
CUSTOM_SCOPE2="CUSTOM_CLAIM2" />
```

**Note:** Claim and scope names are case-sensitive, `CUSTOM_SCOPE1`, and `custom_scope1` are different scopes.

- a. To define scopes with the same spelling but different case, you must use the property subelement. In the following example, the scopes `CUSTOM_SCOPE1` and `custom_scope1` are defined.

```

<scopeToClaimMap CUSTOM_SCOPE1="CUSTOM_CLAIM1, language" >
  <property name="custom_scope1" value="custom_claim1,mobile"/>
</scopeToClaimMap>

```

2. Configure the federated repository properties that are associated with claims. A claim can be mapped to only one federated repository property.

In the following example, the claim CUSTOM\_CLAIM1 is associated with the federated repository property departmentNumber. The claim language is associated with the federated repository property preferredLanguage, and the claim CUSTOM\_CLAIM2 is associated with the federated repository property mail.

```

<claimToUserRegistryMap CUSTOM_CLAIM1="departmentNumber"
  language="preferredLanguage"
  CUSTOM_CLAIM2="mail" />

```

- a. To define claims with the same spelling but different case, you must use the property subelement. In the following example, the claims CUSTOM\_CLAIM1 and custom\_claim1 are defined.

```

<claimToUserRegistryMap CUSTOM_CLAIM1="departmentNumber" >
  <property name="custom_claim1" value="employeeType" />
</claimToUserRegistryMap>

```

3. Configure the user registry attributes that are associated with federated repository properties.

In the following example, the federated repository property photoURL is associated with the LDAP registry attribute ldapPersonPicture

```

<ldapRegistry...>
  ...
  <attributeConfiguration>
    <attribute name="ldapPersonPicture"
      propertyName="photoURL"
      entityType="PersonAccount" />
  </attributeConfiguration>
  ...
</ldapRegistry>

```

**Note:** The LDAP attribute must be defined in the schema of the LDAP registry.

## Results

You have now completed the configuration that is required to customize the claims that are returned by the UserInfo endpoint.

## Configuring an OpenID Connect Provider to enable 2-legged OAuth requests:

8.5.5.4

The typical OAuth flow consists of three “legs”, or stages of interaction between a client and an authorization server. In 2-legged OAuth scenarios, the client uses pre-authorized scopes so that no interaction with the user is necessary, removing the need to perform one of the legs in the typical flow. Specifically, the user does not need to authenticate to the authorization server or give consent for sharing the information that is specified by the requested scopes. Instead, all requested scope parameters are considered pre-authorized and are automatically added to the request token, which is then sent to the authorization server.

### Before you begin

This task expects you to have a Liberty server that is properly configured as an OpenID Connect Provider.

### About this task

In scenarios with two legs or stages, an Open ID Connect client can send a 2-legged HTTP request with a **grant type** of client\_credential or resource owner password. These requests do not go through the

authorization endpoint, so there is no scope consent form for users to confirm and approve the requested scopes; however the OpenID Connect Provider still needs to deal with the authorized scopes in its `access_token` content.

Liberty servers that are configured as OpenID Connect Providers that are equipped to handle 2-legged OAuth requests approve the pre-authorized scopes by using the following criteria:

1. If the **grant\_type** parameter value of a request is `client_credential` or `resource owner password` and the request is an OAuth 2.0 request, then all the scopes that are defined in the request are approved and are copied into the content of the access token. This is the existing behavior of the OAuth 2.0 feature.
2. If the request is an OpenID Connect request or a JWT Token OAuth, or OpenID Connect request, the following criteria is used:
  - If there is no scope parameter that is specified in the request, the OpenID Connect Provider will not accept the request.
  - The requested scopes must be present in the list of scopes that are defined by the scope attribute of the client configuration and must also be specified in the `preAuthorizedScope` list of the client configuration.

This task demonstrates how to configure a Liberty server that is acting as an OpenID Connect Provider to enable 2-legged OAuth requests.

## Procedure

To specify the list of pre-authorized scopes for a client, add the necessary scopes to the `scope` and `preAuthorizedScope` attributes of the client configuration within the appropriate `<oauthProvider>` element in your `server.xml` file. In the example that is shown, the scopes `profile` and `email` are qualified to be specified in the scope list of an access token that is returned by the OpenID Connect Provider. The `phone` scope is not considered a pre-authorized scope because it is missing from the `preAuthorizedScope` list.

```
<oauthProvider id="OAuthConfigSample" ...>
  ....
  <localStore>
    <client name="client01" secret="{xor}..."
      displayName="client01"
      scope="profile email phone"
      preAuthorizedScope="profile email"
      enabled="true"/>
    ....
  </localStore>
</oauthProvider>
```

**Note:** If a requested scope is not listed in the `scope` attribute of the client configuration, it is omitted from the scope of the access token that is returned. If a requested scope is listed in the `scope` attribute of the client configuration but is not included in the `preAuthorizedScope` list of the client configuration, it triggers an `invalid_grant` error in the response from the OpenID Connect Provider.

## Configuring an OpenID Connect Provider to use the RSA-SHA256 algorithm for signing of ID

tokens:  8.5.5.4

You can configure an OpenID Connect Provider to use the RS256 algorithm for the signing of ID tokens.

### About this task

You can configure an OpenID Connect Provider to use the RSA-SHA256 signature algorithm for signing ID tokens by setting the `signatureAlgorithm` to `RS256` and configuring a keystore with the private key used for signing.

## Procedure

1. In the `server.xml` file, create a `keystore` element that refers to the physical keystore that contains the private key that is capable of performing a RSA-SHA256 signature algorithm. For example:  

```
<keystore id="opTestKeyStore" location="{server.config.dir}/opKeyStore.jks" type="JKS" password="keystorePwd" />
```
2. Set the OpenID Connect Provider `signatureAlgorithm` attribute to `RS256`, set the `keyStoreRef` attribute to the `id` value of the keystore element that is used in step 1, and set the `keyAliasName` to locate the private key in the keystore. Setting the `keyStoreRef` is optional if the keystore element `id` used in step 1 is `opKeyStore`. For example:  

```
<openidConnectProvider id="OAuthConfigSample" oauthProviderRef="OAuthConfigSample" signatureAlgorithm="RS256" keyStoreRef="opTestKeyStore" />
```

## Results

You have now configured an OpenID Connect Provider for signing ID tokens with RSA-SHA256.

## Configuring an OpenID Connect Provider to accept JSON Web Tokens (JWT) for authorization

grants:  8.5.5.4

You can configure a Liberty server that acts as an OpenID Connect Provider to accept a JSON Web Token in exchange for an access token.

### About this task

You can configure a Liberty server that acts as an OpenID Connect Provider to accept JSON Web Tokens by enabling the `openidConnectServer-1.0` and `ssl-1.0` features, in addition to other optional configuration information.

## Procedure

1. Ensure the `ssl-1.0` and `openidConnectServer-1.0` features are included in the feature manifest in the `server.xml` file.  

```
<featureManager>  
  <feature>ssl-1.0</feature>  
  <feature>openidConnectServer-1.0</feature>  
</featureManager>
```
2. Optional: Configure a `jwtGrantType` element inside of the appropriate `oauthProvider` element. The `jwtGrantType` element is optional. If no `jwtGrantType` element is included, the default values for all attributes are used; for example:  

```
<oauthProvider id="OAuthConfigSample" ...>  
  <jwtGrantType clockSkew="5m" iatRequired="false" tokenMaxLifetime="120m" maxJtiCacheSize="10000"/>  
  ...  
</oauthProvider>
```

For more JWT configuration options, see the section for the `jwtGrantType` element in the topic.

## Configuring an OpenID Connect Provider to accept client registration requests: 8.5.5.4

The client registration endpoint is an administrator managed service that is used to register, update, delete, and retrieve information about an OpenID Connect Relying Party that intends to use the OpenID Connect Provider. In turn, the registration process can provide information for the Relying Party to use it, including the OAuth 2.0 Client ID and Client Secret, if not specified.

## Before you begin

The client registration service operates in one of two modes: local store or database store. These modes are determined by how the Liberty server configures its client store, whether clients are defined with the `oauthProvider localStore` attributes (local store) in the `server.xml` file or are configured with a database (database store).

In a local store configuration, the client registration service is limited to only retrieving OpenID Connect Relying Party information. You can modify the `server.xml` file to add more operations to register, update, or delete an OpenID Connect Relying Party.

In a database store configuration, there is no limitation on the client registration service and all operations are functional through the REST interface.

**Note:** A Liberty server must not configure its client store with both local store and database store. Choose only one configuration route.

The client registration endpoint is a protected administration endpoint with the `clientManager` role. To access this endpoint, the user must be granted the `clientManager` role by the administrator.

The `clientManager` role is one of the `oauth-roles` defined for an `oauthProvider`. The following is a sample configuration that shows a grant of the `clientManager` role to the user Alice or members in the `clientAdministrator` group.

```
<oauth-roles>
<authenticated>
<special-subject type="ALL_AUTHENTICATED_USERS" />
</authenticated>
<clientManager>
<group name="clientAdministrator" />
<user name="Alice" />
</clientManager>
</oauth-roles>
```

## About this task

Client registration information about an OpenID Connect Relying Party is largely used to define the usage scenario constraints of the client. Additionally, other operations of the OP that are opaque to the client use the client registration metadata to make authorization decisions.

The following example assumes that the Liberty OP is configured with SSL on port 443.

`https://server.example.com:443/oidc/endpoint/<provider_name>/registration`

The previous example also assumes that the `server.xml` file is configured with a user name: `clientAdmin` and password: `clientAdminPassword`, that uses the `oauth-role: clientManager`.

The client registration metadata consists of the following parameters:

*Table 132. Client registration parameters*

Attribute Name	Data Type	Required/Optional	Description
<code>client_id</code>	Input/Output	Optional	The client identifier that is being registered with the OP. Unless specified, this parameter value is generated during registration by default. This is a string.

Table 132. Client registration parameters (continued)

Attribute Name	Data Type	Required/Optional	Description
client_secret	Input/Output	Optional	The client secret that is being registered with the OP. Unless specified, this parameter value is generated during registration by default. This is a string. During an update operation, the parameter value '*' preserves the existing value. A blank parameter value generates a new client_secret. A non-blank parameter value overrides the existing value with the newly specified value.
client_name	Input/Output	Optional	A description for the client that is being registered with the OP. Unless specified, this parameter is set to the client_id parameter value by default. This is a string.
application_type	Input	Optional	The application type that describes the client. Unless specified, the default value is web. This is a string. For example, possible values: <ul style="list-style-type: none"> <li>• &lt;an empty value is valid&gt;</li> <li>• web</li> <li>• native</li> </ul>
response_types	Input	Optional	The response type constraints that are used by this client. Unless specified, the default value is code. This is a JSON array. For example, possible values are: <ul style="list-style-type: none"> <li>• &lt;an empty value is valid&gt;</li> <li>• code</li> <li>• token</li> <li>• id_token token (order reversible)</li> </ul> <p>For a specific response_type, the corresponding grant_types must be specified. For more information, see response_types at the Client Metadata website.</p>

Table 132. Client registration parameters (continued)

Attribute Name	Data Type	Required/Optional	Description
grant_types	Input	Optional	The grant type constraints that are used by this client. Unless specified, the default value is authorization_code. This is a JSON array. For example, the possible values are: <ul style="list-style-type: none"> <li>• &lt;an empty value is valid&gt;</li> <li>• authorization_code</li> <li>• implicit</li> <li>• refresh_token</li> <li>• client_credentials</li> <li>• urn:iETF:params:oauth:grant-type:jwtbearer</li> <li>• password</li> </ul>
redirect_uris	Input	Optional	The array of redirect URIs to which the client is constrained to. This is a JSON array.
post_logout_redirect_uris	Input	Optional	The array of post logout redirect URIs to which the client is constrained. This is a JSON array.
trusted_uri_prefixes	Input	Optional	The array of trusted URI prefixes that the client has deemed safe for sending access tokens. This is a JSON array.
scope	Input	Optional	The space delimited scope values to which the client is constrained. This is a string. If the client is allowed to request any scope, a value of ALL_SCOPES can be used.
preauthorized_scope	Input	Optional	The space delimited scope values that the client is preauthorizing that does not require user consent. This is a string.
subject_type	Input	Optional	The subject type constraint that is described by the client. This is a string. For example, possible values are: <ul style="list-style-type: none"> <li>• &lt;an empty value is valid&gt;</li> <li>• public</li> </ul>

Table 132. Client registration parameters (continued)

Attribute Name	Data Type	Required/Optional	Description
token_endpoint_auth_method	Input	Optional	<p>The token endpoint authentication method constraint that is used by the client. Unless specified, the default value is <code>client_secret_basic</code>. This is a string. For example, possible values are:</p> <ul style="list-style-type: none"> <li>• <code>&lt;an empty value is valid&gt;</code></li> <li>• <code>client_secret_basic</code></li> <li>• <code>client_secret_post</code></li> <li>• <code>none</code></li> </ul>
functional_user_id	Input	Optional	<p>This parameter indicates which user ID to associate with a request made on behalf of a client in a <code>client_credentials</code> grant type. This is a string.</p>
functional_user_groupIds	Input	Optional	<p>A list of group IDs to associate with access tokens obtained by this client using the client credentials grant type. The value is a list of group IDs to which the functional user is a member, where the group IDs are case-sensitive strings. The strings are defined by the authorization server. If the value contains multiple group IDs, their order does not matter. If the list is empty, the claim is omitted. When this client metadata parameter is specified, the value is returned in the <code>functional_user_groupIds</code> response parameter from the introspection endpoint for access tokens that are issued to this client with a client credentials grant. If the <code>functional_user_id</code> parameter is not used, this parameter is ignored.  <b>Note:</b> Authorization Servers must not trust the client to self-assert this parameter.</p>

Table 132. Client registration parameters (continued)

Attribute Name	Data Type	Required/Optional	Description
introspect_tokens	Input	Optional	A parameter value that indicates whether the specified client has the privilege to introspect an access token that is issued by the OP. This is a Boolean value.
registration_client_uri	Output only	N/A	A parameter that is returned in a response with the value that indicates the unique URL for a registered client. This is a string.
client_secret_expires_at	Output only	N/A	A parameter that is returned in a response with the value that indicates the number of seconds from 1970-01-01T0:0:0Z as measured in UTC, at which the client secret expires. The value 0 indicates no expiration time.
client_id_issued_at	Output only	N/A	A parameter that is returned in a response with the value that indicates the number of seconds from 1970-01-01T0:0:0Z as measured in UTC, at which the client ID was issued. The value 0 indicates that no client ID issue time was identified.

## Procedure

1. Register a client, as shown in the following example:

Request Headers:

```
POST https://server.example.com:443/oidc/endpoint/<provider_name>/registration
Accept: application/json
Content-Type: application/json
Authorization: Basic Y2xpZW50QWRtaW46Y2xpZW50QWRtaW5QYXNzd29yZA==
```

Request Payload:

```
{
  "token_endpoint_auth_method": "client_secret_basic",
  "scope": "openid profile email general",
  "grant_types": [
    "authorization_code",
    "client_credentials",
    "implicit",
    "refresh_token",
    "urn:iETF:params:oauth:grant-type:jwt-bearer"
  ],
  "response_types": [
    "code",
    "token",
    "id_token token"
  ],
}
```

```

"application_type":"web",
"subject_type":"public",
"post_logout_redirect_uris":[
  "https://server.example.com:9000/logout/",
  "https://server.example.com:9001/exit/"
],
"preauthorized_scope":"openid profile email general",
"introspect_tokens":true,
"trusted_uri_prefixes":[
  "https://server.example.com:9000/trusted/"
],
"redirect_uris":[
  "https://server.example.com:443/resource/redirect1",
  "https://server.example.com:9000/resource/redirect2"
]
}

```

#### Response Headers:

```

Status: 201
Cache-Control: private
ETag: "1B2M2Y8AsgTpgAmY7PhCfg=="
Content-Type: application/json

```

#### Response Body:

```

{
  "client_id_issued_at":1401776782,
  "registration_client_uri":"https://server.example.com:8020/oidc/endpoint/OIDC/registration/b0a376ec4b694b67b6baeb0",
  "client_secret_expires_at":0,
  "token_endpoint_auth_method":"client_secret_basic",
  "scope":"openid profile email general",
  "grant_types":[
    "authorization_code",
    "client_credentials",
    "implicit",
    "refresh_token",
    "urn:iETF:params:oauth:grant-type:jwt-bearer"
  ],
  "response_types":[
    "code",
    "token",
    "id_token token"
  ],
  "application_type":"web",
  "subject_type":"public",
  "post_logout_redirect_uris":[
    "https://server.example.com:9000/logout/",
    "https://server.example.com:9001/exit/"
  ],
  "preauthorized_scope":"openid profile email general",
  "introspect_tokens":true,
  "trusted_uri_prefixes":[
    "https://server.example.com:9000/trusted/"
  ],
  "client_id":"b0a376ec4b694b67b6baeb0604a312d8",
  "client_secret":"nmr0Q20CrMdw4pjqaimutZTcbQPzIoYgItjaccb9Wk33rKarhM3WDLmWIoE",
  "client_name":"b0a376ec4b694b67b6baeb0604a312d8",
  "redirect_uris":[
    "https://server.example.com:443/resource/redirect1",
    "https://server.example.com:9000/resource/redirect2"
  ]
}

```

2. Update a client, as shown in the following example:

#### Request Headers:

PUT https://server.example.com:443/oidc/endpoint/<provider\_name>/registration/registration/b0a376ec4b694b67b6baeb0604a312d8  
Accept: application/json  
Content-Type: application/json  
Authorization: Basic Y2xpZW50QRtaW46Y2xpZW50QRtaW5QYXNzd29yZA==

Request Payload:

```
{
  "token_endpoint_auth_method": "client_secret_basic",
  "scope": "openid profile",
  "grant_types": [
    "authorization_code"
  ],
  "response_types": [
    "code"
  ],
  "application_type": "native",
  "subject_type": "public",
  "post_logout_redirect_uris": [
    "https://server.example.com:9000/logout/"
  ],
  "preauthorized_scope": "openid",
  "introspect_tokens": false,
  "trusted_uri_prefixes": [
    "https://server.example.com:9003/trusted/"
  ],
  "client_id": "b0a376ec4b694b67b6baeb0604a312d8",
  "client_secret": "*",
  "client_name": "updated client",
  "redirect_uris": [
    "https://server.example.com:443/resource/redirect1"
  ]
}
```

Response Headers:

Status: 200  
ETag: "3DD7affTGS91mfhPZ83B39Y=="  
Content-Type: application/json

Response Body:

```
{
  "client_id_issued_at": 1401776782,
  "registration_client_uri": "https://server.example.com:8020/oidc/endpoint/OIDC/registration/b0a376ec4b694b67b6baeb0604a312d8",
  "client_secret_expires_at": 0,
  "token_endpoint_auth_method": "client_secret_basic",
  "scope": "openid profile",
  "grant_types": [
    "authorization_code"
  ],
  "response_types": [
    "code"
  ],
  "application_type": "native",
  "subject_type": "public",
  "post_logout_redirect_uris": [
    "https://server.example.com:9000/logout/"
  ],
  "preauthorized_scope": "openid",
  "introspect_tokens": false,
  "trusted_uri_prefixes": [
    "https://server.example.com:9003/trusted/"
  ],
  "client_id": "b0a376ec4b694b67b6baeb0604a312d8",
  "client_secret": "*",
  "client_name": "updated client",
}
```

```

    "redirect_uris":[
      "https://server.example.com:443/resource/redirect1"
    ]
  }
}

```

3. Retrieve a client, as shown in the following example:

**Request Headers:**

```

GET https://server.example.com:443/oidc/endpoint/<provider_name>/registration/registration/b0a376ec4b694b67b6baeb0604a312d8
Accept: application/json
Authorization: Basic Y2xpZW50QWRtaW46Y2xpZW50QWRtaW5QYXNzd29yZA==

```

**Response Headers:**

```

Status: 200
Cache-Control: private
ETag: "3DD7affTGS91mfhPZ83B39Y=="
Content-Type: application/json

```

**Response Body:**

```

{
  "client_id_issued_at":1401776782,
  "registration_client_uri":"https://server.example.com:8020/oidc/endpoint/OIDC/registration/b0a376ec4b694b67b6baeb0604a312d8",
  "client_secret_expires_at":0,
  "token_endpoint_auth_method":"client_secret_basic",
  "scope":"openid profile",
  "grant_types":[
    "authorization_code"
  ],
  "response_types":[
    "code"
  ],
  "application_type":"native",
  "subject_type":"public",
  "post_logout_redirect_uris":[
    "https://server.example.com:9000/logout/"
  ],
  "preauthorized_scope":"openid",
  "introspect_tokens":false,
  "trusted_uri_prefixes":[
    "https://server.example.com:9003/trusted/"
  ],
  "client_id":"b0a376ec4b694b67b6baeb0604a312d8",
  "client_secret":"*",
  "client_name":"updated client",
  "redirect_uris":[
    "https://server.example.com:443/resource/redirect1"
  ]
}

```

4. Retrieve a client (head request), as shown in the following example:

**Request Headers:**

```

HEAD https://server.example.com:443/oidc/endpoint/<provider_name>/registration/registration/b0a376ec4b694b67b6baeb0604a312d8
Accept: application/json
Authorization: Basic Y2xpZW50QWRtaW46Y2xpZW50QWRtaW5QYXNzd29yZA==

```

**Response Headers:**

```

Status: 200
Cache-Control: private, no-cache=set-cookie
ETag: "3DD7affTGS91mfhPZ83B39Y=="
Content-Type: application/json

```

5. Delete a client, as shown in the following example:

**Request Headers:**

```

DELETE https://server.example.com:443/oidc/endpoint/<provider_name>/registration/registration/b0a376ec4b694b67b6baeb0604a312d8
Authorization: Basic Y2xpZW50QWRtaW46Y2xpZW50QWRtaW5QYXNzd29yZA==

```

**Response Headers:**

Status: 204  
Content-Length: 0  
Content-Language: en-US

**Note:** The information in this topic also applies to client registration services of OAuth 2.0 clients, and OpenID Connect Relying parties.

### OpenID Connect custom forms: 8.5.5.4

You can replace the default form login page for user authentication, or develop your own user consent form to collect client authorization data.

### Authenticating a user: 8.5.5.4

OpenID Connect provider supports traditional Java Platform, Enterprise Edition (J2EE) FormLogin for user authentication.

You can customize the login form, see  8.5.5.4 OpenID Connect custom forms.

The OpenID Connect provider can be configured to support other authentication methods.

### OpenId Connect provider delegates user authentication to third-party authentication service

If you configure Trust Association Interceptor (TAI) to intercept a request to an OpenID Connect authorization endpoint (`/oidc/<provider name>/authorize`), the login form is not presented, and the user authentication is performed by the configured TAI.

### OpenId Connect provider authenticates user with HTTP Basic Authentication

If you want an OpenID Connect provider to authenticate a user with HTTP Basic Authentication, the openid connect authorization request must include a user id and password as defined in the Basic Authentication Scheme.

### OpenID Connect provider authenticates user with a client certificate

If you want an OpenID Connect provider to authenticate a user with a client certificate, you need to explicitly add the attribute `certAuthentication=true` inside the `oauthProvider` configuration element that is referenced by the `openidConnectProvider` configuration, and the user agent must be able to provide a client certificate for an OpenID Connect authorization request.

### OpenId Connect provider delegates user authentication to a third-party OpenId Connect provider

You can configure an OpenID Connect provider to delegate user authentication to a third-party OpenID Connect provider. To enable this authentication delegation, you configure the OP as an OpenID Connect relying party. Optionally, you can add an authentication filter to limit the `openidConnectClient-1.0` feature to protect an OpenID Connect authorization endpoint (`/oidc/<provider name>/authorize`) only.

## Configuring an OpenID Connect Client in Liberty

### 8.5.5.4

You can configure a Liberty server to function as an OpenID Connect Client, or Relying Party, to take advantage of web single sign-on and to use an OpenID Connect Provider as an identity provider.

## About this task

You can configure a Liberty server to act as an OpenID Connect Client by enabling the `openidConnectClient-1.0` feature in Liberty, and in addition to other configuration information.

## Procedure

1. Add the `openidConnectClient-1.0` Liberty feature and any other needed features to the `server.xml` file. The `ssl-1.0` feature is also required for the `openidConnectClient-1.0` feature. Add the following element declaration inside the `featureManager` element in your `server.xml` file:

```
<feature>openidConnectClient-1.0</feature>
<feature>ssl-1.0</feature>
```

2. Configure an `openidConnectClient` element. The following is an example of a minimal configuration that works with the default Liberty server OpenID Connect Provider.

The client must have a configured application available at the given URL pattern that can handle redirect requests from an OpenID Connect Provider. This URL must also precisely match the redirect URL registered for the client with the OP.

**Avoid trouble:** In this example, the client expects the SSL port to be set to 443.

```
<openidConnectClient id="client01"
  clientId="client01"
  clientSecret="{xor}LDo8LTor"
  authorizationEndpointUrl="https://server.example.com:443/oidc/endpoint/OidcConfigSample/authorize"
  tokenEndpointUrl="https://server.example.com:443/oidc/endpoint/OidcConfigSample/token">
</openidConnectClient>
```

In this sample minimal configuration, the following default values are assumed:

- `scope=openid profile`: The scope of `openid` is required, and you can use the `scope` attribute to edit required scopes. For example, you can change the required scope to `openid profile email`.
  - This RP registers its redirect URL with the OP as `https://<host name>:<ssl port>/oidcclient/redirect/client01`, where both the host name and ssl port are automatically resolved, and `client01` is the ID of the `openidConnectClient` configuration element. If there is a proxy in front of the RP, you can override the host name and port with the attribute `redirectToRPHostAndPort`, and set `redirectToRPHostAndPort` to `https://<host name>:<ssl port>`.
3. Configure a user registry. User identities that are returned by the OP are not mapped to a registry user by default, so no users are required to be configured in the registry. However, if the `mapIdentityToRegistryUser` attribute of the `openidConnectClient` element is set to `true`, there must be a user entry for the appropriate identity that is returned from the OP in order for authentication and authorization to succeed. For more information about configuring a user registry, see “Configuring a user registry for Liberty” on page 1851.
  4. Configure the truststore of the server to include the signer certificates of the OpenID Connect Providers that are supported. For information about keystores, see “Enabling SSL communication in Liberty” on page 1834.
  5. Modify the SSL configuration of the server to use the configured truststore.

```
<sslDefault sslRef="DefaultSSLSettings" />
<ssl id="DefaultSSLSettings" keyStoreRef="myKeyStore" trustStoreRef="myTrustStore" />
<keyStore id="myKeyStore" password="{xor}EzY90i0rJg==" type="jks" location="{server.config.dir}/resources/security/
<keyStore id="myTrustStore" password="{xor}EzY90i0rJg==" type="jks" location="{server.config.dir}/resources/security/
```

OpenID Connect is configured to use the default SSL configuration that is specified by the server. Therefore, the default SSL configuration for the server must use the truststore that is configured for OpenID Connect.

6. **8.5.5.5** Optional: Configure a third party OpenID Connect provider.

To configure the Liberty OpenID Connect client to use a third party OpenID Connect Provider such as (Microsoft Azure or Google), you must configure the following attributes. The attribute values can be obtained by calling the OP's discovery endpoint, which provides a JSON document at the path that is formed by concatenating the string `/.well-known/openid-configuration` to the issuer.

- a. Set the `jwkEndpointUrl` attribute to the URL of the OP's JSON Web Key Set JWK document that is defined as `asjwks_uri` in the discovery file. For example, to use Google's OP, you can set `jwkEndpointUrl = "https://www.googleapis.com/oauth2/v2/certs"`.
- b. Set the `issuerIdentifier` attribute to the issuer as defined in the discovery file. An ID Token that does not contain this value as an `iss` claim is rejected. For example, you can set `issuerIdentifier="accounts.google.com"` if you are using Google as your OP.
- c. Set `signatureAlgorithm="RS256"`. The Liberty OpenID Connect client's default signature algorithm is HS256.
- d. Set the `userIdentityToCreateSubject` attribute to a claim name used by the vendor's ID Token that represents a user's unique identifier. For example, you can set `userIdentityToCreateSubject="email"` if you are using Google's OP, and `userIdentityToCreateSubject="upn"` or `userIdentityToCreateSubject="unique_name"` if you are using Microsoft Azure.
- e. Set the `groupIdentifier` attribute to the claim name that represents the user's group memberships or roles. For example, you can set `groupIdentifier="groups"` if you are using Microsoft Azure.

For more OpenID Connect Client configuration options, see .

#### 7. Optional: Authentication Filter.

When the `openidConnectClient-1.0` feature is enabled and the `openidConnectClient` element is not configured with an `authFilterRef` attribute, any unauthenticated request is authenticated through the OpenID Connect provider.

For more information on configuring the authentication filter, see  [“Authentication Filters”](#) on page 1937.

#### 8. Support multiple OpenID Connect Providers.

You can configure Liberty as an OpenID Connect Relying Party to multiple OpenID Connect Providers by creating multiple `openidConnectClient` elements and multiple Authentication Filters. Each `openidConnectClient` element defines one Single-Sign-On relationship with one OpenID Connect Provider, and use the `authFilterRef` attribute to reference to one Authentication Filter.

#### 9. Configure a supported ID Token signature algorithm.

You can configure a Liberty OpenID Connect client to support the RS256 signature algorithm in an ID Token. The Liberty OpenID Connect client's default signature algorithm is HS256. If you configure RS256 as the ID Token's signature algorithm by setting `signatureAlgorithm="RS256"`, you must configure both the `trustStoreRef` and `trustAliasName`, unless the OP supports a JWK endpoint.

#### 10. Optional: Configure an “implicit” grant type.

The `openidConnectClient-1.0` feature uses an Authorization Code grant type to request a user authentication token, and you can configure the Liberty `openidConnectClient-1.0` feature to use an “implicit” grant type by adding `grantType="implicit"` to the `server.xml` file. If your Liberty server and OpenID Connect provider are in different firewalls, you must use this configuration option.

## Results

You have now established the minimum configuration that is required to configure a Liberty server as an OpenID Connect Client capable of communicating with other Liberty servers configured as OpenID Connect Providers.

### Invoking the Authorization Endpoint for OpenID Connect: [8.5.5.4](#)

In OpenID Connect the authorization endpoint handles authentication and authorization of a user.

## Before you begin

When starting the authorization endpoint from an in-browser client application or a client application implemented in a scripting language such as Javascript, for example, no configuration of a Liberty server as an OpenID Connect Client is necessary.

## About this task

The authorization endpoint accepts an authentication request that includes parameters that are defined by both the OAuth 2.0 and OpenID Connect 1.0 specifications.

In the Authorization Code Flow, the authorization endpoint is used for authentication and authorization and returns an authorization grant to the client. This authorization grant can then be passed in a request by the client to the token endpoint in exchange for an ID token, access token, and refresh token. In the Implicit Flow, the authorization endpoint still performs authentication and authorization but also directly returns an ID token and access token to the client in its response; no interaction is performed with the token endpoint.

A Liberty server with OpenID Connect enabled has access to the OpenID Connect authorization endpoint at the following URL:

```
https://server.example.com:443/oidc/endpoint/<provider_name>/authorize
```

**Avoid trouble:** In this example, the client expects the SSL port to be set to 443.

## Procedure

1. Prepare an HTTP GET or POST request that includes the following required and recommended parameters.
  - **scope:** (Required) OpenID Connect requests must contain the `openid` scope value. Other scopes may also be present
  - **response\_type:** (Required) Determines the authorization processing flow to be used. When using the Authorization Code Flow, this value is `code`. When using the Implicit Flow, this value is `id_token` token or `id_token`. No access token is returned when the value is `id_token`
  - **client\_id:** (Required) Client identifier that is valid at the OpenID Connect Provider.
  - **redirect\_uri:** (Required) Redirection URI to which the response will be sent. This value must exactly match one of the redirection URI values for the registered client at the OP.
  - **state:** (Recommended) Opaque value used to maintain state between the request and the callback.
  - **nonce:** (Required for the Implicit Flow) String value used to associate a client session with an ID token and to mitigate replay attacks.

You can include more parameters in the request. For a description of other supported parameters, see the OpenID Connect Core 1.0 specification.

We do not support only an `id_token` `response_type`. Using the implicit flow must always use `id_token` token and will return an access token.

2. Send the GET or POST request to the authorization endpoint URL.

## Results

After completing these steps, you have a valid HTTP request that is being sent to the authorization endpoint. The authorization endpoint returns a response in the manner described in the Examples section.

The OpenID Connect Provider attempts to authenticate and authorize the user once it receives a request from the client.

In the Authorization Code Flow, if authentication and authorization succeed, the OpenID Connect Provider issues an authorization code and includes it as a parameter in an OAuth 2.0 Authorization Response to the client. If the initial request included **state**, the authorization response will also include the exact **state** value that was included in the initial request. Using the application/x-www-form-urlencoded format, the **code** and **state** parameters are added as query parameters to the **redirect\_uri** value that was specified in the authorization request.

In the Implicit Flow, if authentication and authorization succeed, the following parameters are returned from the authorization endpoint.

- **access\_token**: Access token. This is returned unless the **[response\_type]** value in the initial request is **[id\_token]**.
- **token\_type**: OAuth 2.0 Token Type. For OpenID Connect, this value is Bearer.
- **id\_token**: ID token.
- **state**: Required if included in authorization request.
- **expires\_in**: (Optional) Expiration time of the access token in seconds since the response was generated.

These parameters are added to the fragment component of the **redirect\_uri** value that is specified in the authorization request, not as query parameters such as in the Authorization Code Flow.

## Example

The following examples show forms of Authorization and Implicit code flow.

An example request for the Authorization Code Flow is shown here:

```
GET /authorize?  
  response_type=code  
  &scope=openid profile email  
  &client_id=client01  
  &state=af0ifjsldkj  
  &redirect_uri=https://server.example.com:443/oidcclient/redirect/client01 HTTP/1.1
```

An example request for the Implicit Flow is shown here:

```
GET /authorize?  
  response_type=id_token token  
  &scope=openid profile  
  &client_id=client01  
  &state=af0ifjsldkj  
  &redirect_uri=https://server.example.com:443/oidcclient/redirect/client01  
  &nonce=n-0S6_wzA2Mj HTTP/1.1
```

An example response from the authorization endpoint in the Authorization Code Flow is shown here:

```
HTTP/1.1 302 Found  
Location: https://server.example.com:443/oidcclient/redirect/client01  
  code=Sp1x10BeZQQYbYS6WxSbIA  
  &state=af0ifjsldkj
```

An example response from the authorization endpoint in the Implicit Flow is shown here:

```
HTTP/1.1 302 Found  
Location: https://server.example.com:443/oidcclient/redirect/client01  
  access_token=S1AV32hkKG  
  &token_type=Bearer  
  &id_token=eyJ0 ... NiJ9.eyJ1c ... I6IjIifX0.DeWt4Qu ... ZXso  
  &expires_in=3600  
  &state=af0ifjsldkj
```

## Invoking the Token Endpoint for OpenID Connect: 8.5.5.4

In the OpenID Connect Authorization Code Flow, the token endpoint is used by a client to obtain an ID token, access token, and refresh token.

### Before you begin

When starting the token endpoint from an in-browser client application or a client application implemented in a scripting language such as Javascript, for example, no configuration of a Liberty server as an OpenID Connect Client is necessary.

### About this task

The token endpoint accepts a request from the client that includes an authorization code that is issued to the client by the authorization endpoint. When the authorization code is validated, the appropriate tokens are returned in a response to the client.

The token endpoint is not used in the OpenID Connect Implicit Flow.

A Liberty server with OpenID Connect enabled has access to the OpenID Connect token endpoint at the following URL:

```
https://server.example.com:443/oidc/endpoint/<provider_name>/token
```

**Avoid trouble:** In this example, the client expects the SSL port to be set to 443. All communication with the token endpoint must use TLS.

### Procedure

1. Prepare an HTTP POST request with the following parameters.
  - **grant\_type:** The value of this parameter must be `authorization_code`.
  - **code:** The authorization code received from the authorization endpoint.The parameters must be added by using the `application/x-www-form-urlencoded` format.
2. POST the request to the token endpoint URL.

### Results

After completing these steps you have a valid HTTP POST request that is being sent to the token endpoint. The token endpoint returns a response as described in the Examples section.

When the OpenID Connect Provider validates the token request that is received from the client, the OpenID Connect Provider returns an HTTP 200 response back to the client with a JSON object in `application/json` format. The response includes the ID token, access token, and refresh token, along with the following additional parameters:

- **token\_type:** OAuth 2.0 Token Type. For OpenID Connect, this value is `Bearer`.
- **expires\_in:** Expiration time of the access token in seconds since the response was generated.

All responses from the token endpoint that contain tokens, secrets, or other sensitive information have their **Cache-Control** header value set to **no-store** and **Pragma** header value set to **no-cache**.

## Example

The following shows examples of an HTTP POST request and response

An example request is shown here:

```
POST /token HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
    grant_type=authorization_code
    &code=Sp1x10BeZQYbYS6WxSbIA
    &redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb
```

An example response is shown here:

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache
{
  "access_token": "S1AV32hkKG",
  "token_type": "Bearer",
  "refresh_token": "8xL0xBtZp8",
  "expires_in": 3600,
  "id_token": "eyJ ... zcifQ.ewo ... NzAKfQ.ggW8h ... Mzqg"
}
```

## Invoking the Introspection Endpoint for OpenID Connect:



8.5.5.4

The introspection endpoint enables holders of access tokens to request a set of metadata about an access token from the OpenID Connect Provider that issued the access token. The access token must be one that was obtained through OpenID Connect or OAuth authentication.

### Before you begin

When a resource service or a client application invokes the introspection endpoint, it must register itself as a normal OAuth 2.0 client to the OpenID Connect server. The registered client metadata must include the attribute `introspectTokens = true`.

### About this task

Information that is contained within access tokens that are used in OpenID Connect and OAuth 2.0 is opaque to clients. This can enable protected resources or clients to make authorization decisions that are based on the metadata that is returned from the OpenID Connect Provider about the access token.

A Liberty server with OpenID Connect enabled has access to the OpenID Connect introspection endpoint at the following URL:

```
https://server.example.com:443/oidc/endpoint/<provider_name>/introspect
```

**Avoid trouble:** In this example, the client expects the SSL port to be set to 443.

### Procedure

1. Set up client authentication with the client ID and password for a registered OpenID Connect Client in the HTTP Basic Authorization header of a GET or POST request. The client ID and password are encoded by using the `application/x-www-form-urlencoded` encoding algorithm. The encoded client ID is used as the username and the encoded password is used as the password.
2. Include the string value for the access token as a parameter in the GET or POST request to the introspection endpoint.
3. Send the GET or POST request to the introspection endpoint URL.

## Results

After completing these steps you have a valid HTTP request that is being sent to the introspection endpoint as shown in the Examples section.

For valid requests, the introspection endpoint returns an HTTP 200 response with a JSON object in application/json format that includes the following information, depending upon whether the access token is active or expired.

When the access token is active, the endpoint returns active:true, as well as the following additional information in the JSON object:

**active** Boolean indicator of whether the access token is active.

**client\_id**

Client identifier of the OpenID Connect Client who requested the access token.

**sub** Resource owner who authorized the access token.

**scope** Space-separated list of scopes that are associated with the access token.

**iat** Integer timestamp, measured in seconds since January 1, 1970 UTC, indicating when the access token was issued.

**exp** Integer timestamp, measured in seconds since January 1, 1970 UTC, indicating when the access token will expire.

**realmName**

Realm name of the resource owner.

**uniqueSecurityName**

Unique security name of the resource owner.

**tokenType**

Access token type. For OpenID Connect, this value is Bearer.

**grant\_type**

String indicating the type of grant that generated the access token. Possible values are: authorization\_code, password, refresh\_token, client\_credentials, resource\_owner, implicit, and urn:iETF:params:oauth:grant-type:jwt-bearer.

If the access token is expired, but the provided authentication is valid, or if the provided access token is of the wrong type, the endpoint returns active:false in the JSON object.

**Note:** For a client or resource service to perform access token introspection, the client or resource service must register itself as a client to the OpenID Connect provider, and the client metadata must have introspect\_tokens set to true.

## Example

The following shows examples of an active and expired access token along with a request.

An example request is shown here:

```
POST /register HTTP/1.1
Accept: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0Mzo3RmpmcDBaQnIxS3REUmJuZlZkbU13
token=SOYleDziTitHeKcodp6vqEmRwKPjz31FZTcsQtVC
```

An example response for an active access token:

```

HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
{
  "exp"           : 1415307710,
  "realmName"    : "BasicRealm",
  "sub"          : "testuser",
  "scope"        : "openid scope2 scope1",
  "grant_type"   : "authorization_code",
  "uniqueSecurityName" : "testuser",
  "active"       : true,
  "token_type"   : "Bearer",
  "client_id"    : "pclient01",
  "iat"          : 1415307700
}

```

Example response for an expired access token:

```

HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
{
  "active":"false"
}

```

## Invoking the coverage map service: 8.5.5.4

The coverage map service is an unprotected endpoint that returns a JavaScript Object Notation (JSON) array of slash-terminated URI prefixes. The array of URI prefixes designates which web contexts are part of a Single Sign On (SSO) group, thus enabling clients to know whether a URI destination is deemed safe to send an access token.

### Before you begin

The coverage map service returns a JSON array of URI prefixes, which are a unique set that is derived from the aggregation of the **trusted\_uri\_prefixes** parameter values that are specified in the registered clients. Therefore, a typical case for populating the coverage map service is to register clients and specify the **trusted\_uri\_prefixes** value.

### About this task

The following example assumes that the Liberty OpenID Connect provider is configured with SSL on port 443.

```
https://server.example.com:443/oidc/endpoint/<provider_name>/coverage_map
```

Additionally, this example assumes that a client is registered with the specified **trusted\_uri\_prefixes**.

### Procedure

1. Specify a **token\_type URI** query parameter on the coverage\_map endpoint. The following is an example request that assumes that the client is registered with the specified trusted\_uri\_prefixes  

```
https://server.example.com:443/oidc/endpoint/<provider_name>/coverage_map?token_type=bearer
```

The only token\_type value that is supported is **token\_type=bearer**.
2. Get the coverage map for the bearer token type, as shown in the following example.  

Request Headers:

```
GET https://server.example.com:443/oidc/endpoint/<provider_name>/coverage_map?token_type=bearer
```

Response Headers:

```
Status: 200
CacheControl: public, maxage=600
ETag:"vvhkgXkRx+BzR3Q4kwCCqw=="
ContentType: application/json

Response Body:
[
  "http://res1.ibm.com/",
  "https://trusted.server.ibm.com:9554/resources/"
]
```

## Invoking the UserInfo Endpoint for OpenID Connect: 8.5.5.4

The UserInfo endpoint returns claims about a user that is authenticated with OpenID Connect authentication.

### About this task

To obtain the claims for a user, a client makes a request to the UserInfo endpoint by using an access token as the credential. The access token must be one that was obtained through OpenID Connect authentication. The claims for the user who is represented by the access token are returned as a JSON object that contains a collection of name-value pairs for the claims. The UserInfo endpoint is an OAuth 2.0 protected resource, which means that the credential required to access the endpoint is the access token.

The claims that are returned by the UserInfo endpoint can be customized with the OpenID Connect Provider configuration, see [Configuring claims returned by the UserInfo endpoint](#).

A Liberty profile server with OpenID Connect enabled has access to the OpenID Connect UserInfo endpoint at the following URL:

```
https://server.example.com:443/oidc/endpoint/<provider_name>/userinfo
```

**Avoid trouble:** In this example, the client expects the SSL port to be set to 443.

### Procedure

1. Set up authentication with an access token that was obtained through OpenID Connect authentication. The access token can be provided in the HTTP Basic Authorization header or with the `access_token` request parameter. In either case, the access token does not need to be encoded.
2. Send the GET or POST request to the UserInfo endpoint URL.

### Results

After completing these steps you have a valid HTTP request that is being sent to the UserInfo endpoint as shown in the Examples section.

For valid requests, the UserInfo endpoint returns an HTTP 200 response with a JSON object in `application/json` format that includes the claims that are configured for the OpenID Connect Provider.

### Example

The following examples illustrate requests with a valid token and invalid tokens.

- Request that uses the HTTP Bearer Authorization header to pass the access token
- Response for a valid access token
- Invalid access tokens

An example request that uses the HTTP Bearer Authorization header to pass the access token:

```
POST /register HTTP/1.1
Accept: application/x-www-form-urlencoded
Authorization: Bearer fAAAdL01c6QWDbPs9HrWHz5e7nRWVAnxqTTP7i88G
```

The token can also be passed by using the `access_token` request parameter:

```
POST /register HTTP/1.1
Accept: application/x-www-form-urlencoded
access_token=fAAAdL01c6QWDbPs9HrWHz5e7nRWVAnxqTTP7i88G
```

It is a best practice to use the HTTP Authorization header instead of the `access_token` request parameter because HTTP request parameters, which can include sensitive information, can be saved in the browser history or cache.

Here is an example response for a valid access token. The `sub` and `groupIds` claims are always returned. The other claims that are shown here are the default claims for an OpenID Connect Provider.

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache
{
  "sub"      : "bob",
  "groupIds" : [ "bobsdepartment","administrators" ],
  "given_name" : "Bob",
  "name"      : "Bob Smith",
  "email"     : "bob@mycompany.com",
  "phone_number" : "+1 (604) 555-1234;ext5678",
  "address"   : { "formatted" : "123 Main St., Anytown, TX 77777" },
  "picture"   : "http://mycompany.com/bob_photo.jpg"
}
```

For an invalid access token, the `UserInfo` endpoint returns an HTTP 401 status code with an error message in the `WWW-AUTHENTICATE` header.

```
HTTP/1.1 401 Unauthorized
CONTENT-LENGTH : 0
WWW-AUTHENTICATE : Bearer error=invalid_token,
  error_description=CWwKS1617E: A userinfo request was made with
  an access token that was not recognized. The request URI was
  /oidc/endpoint/MyOAuthProvider/userinfo.
```

## Invoking the Session Management Endpoint for OpenID Connect:

8.5.5.4

The session management endpoint enables OpenID Connect Relying Parties to monitor the login status of a user with a particular OpenID Connect Provider (OP) while minimizing network traffic. With the help of the session management endpoint, a Relying Party (RP) can log out a user who logged out of the OpenID Connect Provider.

### Before you begin

The OP session management endpoint URL is obtained from the `check_session_iframe` attribute in the discovery information that is returned from the discovery endpoint of the OP. This URL must be used as the target of an `iframe` in the RP application that requires session management functionality. The RP application must also know the `id` attribute of the `iframe` in order to submit `Window.postMessage()` requests to it.

### About this task

To help determine the login status of a user, the RP loads an `iframe` with its `src` target set to the session management endpoint of the OP. The session management endpoint has access to a cookie that stores the login status, or browser state, of a user. This browser state cookie is updated when a user logs out of the

OP. The RP can then use client side scripting to invoke the `Window.postMessage()` function of the OP iframe, sending the client ID and the currently known session state in the text of the message. If the RP receives a `postMessage` back from the OP frame with a value of `changed`, then the login status of the user at the OP has changed and the RP can decide whether to log out the user. If a value of `unchanged` is returned, the user is still logged in at the OP.

A Liberty server with OpenID Connect enabled has access to the OpenID Connect session management endpoint at the following URL:

```
https://server.example.com:443/oidc/endpoint/<provider_name>/check_session_iframe
```

**Avoid trouble:** In this example, the client expects the SSL port to be set to 443.

### Procedure

1. Create a web resource in an appropriate RP application capable of loading an iframe that targets the OP session management endpoint. The web resource also needs to have access to the session state value that is returned in the `session_state` parameter of the authorization response. The session state value can be stored in a cookie, for example, or in any other way that allows client-side scripting in the web resource to know what the value is. The following is a sample HTML snippet for such an iframe.

```
<iframe id="iframeOP" src="https://server.example.com:443/oidc/endpoint/0idcConfigSample/check_session_iframe" frameborder="0"></iframe>
```

2. To check the login status of a user, invoke the `Window.postMessage()` function of the OP iframe, passing the client ID and session state as the message parameter in the format `Client ID + " " + Session State` and the host name of the OP as the target origin parameter. In the following JavaScript sample function, the script expects the session state value to be stored in a cookie that is named `session_state`, and the `getCookieValue()` function returns the value that is stored in the `session_state` cookie.

```
var targetOP = "https://server.example.com:443";
function checkStatus() {
    var client = "client01";
    var sessionState = getCookieValue("session_state");
    var text = client + " " + sessionState;
    var iframe = document.getElementById("iframeOP");
    iframe.contentWindow.postMessage(text, targetOP);
}
```

3. Configure the web resource to listen for `postMessages` from the OP that contain the value `changed` or `unchanged` to reflect the respective login status of the user. The RP can then decide whether to log the user out of the RP based on the value that is returned from the OP. The function must ensure that the origin of the `postMessage` matches the expected OP host name. Any messages that do not match are rejected. The following JavaScript example shows how to add an event listener to the web resource to listen for such messages.

```
var targetOP = "https://server.example.com:443";
window.addEventListener("message", receiveMessage, false);
function receiveMessage(event) {
    if (event.origin !== targetOP) {
        // Origin did not come from the OP; this message must be rejected.
        return;
    }
    if (event.data === "unchanged") {
        // User is still logged in to the OP
    } else {
        // User has logged out of the OP
    }
}
```

### Results

You now have a web resource on the RP that is capable of utilizing the session management functionality of OpenID Connect on a Liberty server OP. The browser state that is maintained in the OP iframe is

updated when users log in or log out of the OP. After successful login at the OP, a new session state value is provided in the authorization response to the RP. The RP can then use client-side scripting to validate the session state of the user to determine whether the login status of the user changed on the OP without broadcasting extra network traffic.

## Example

The following HTML example shows a complete HTML page that uses OpenID Connect Session Management. The src attribute of the OP iframe is set to the session management endpoint URL obtained from the OP. The startChecking() function is automatically called every 60 seconds and checks the login status of the user. The page has a message event listener that calls the receiveMessage() function when a postMessage is received. This function makes sure the postMessage comes from the expected domain for the OP and checks the value of the returned message to see whether the login status of the user is changed or unchanged.

You can load this HTML page, itself, as an invisible iframe in another web resource within the RP. This enables any web resource that loads this iframe to monitor the login status of the user on the client side.

```
<!DOCTYPE html>
<html>
<head>
<meta charset="ISO-8859-1">
<title>iFrame RP Page</title>
</head>
<body onload="javascript:startChecking()">
  <iframe id="iframeOP" src="https://localhost:8999/oidc/endpoint/OidcConfigSample/check_session_iframe" frameborder="0">
</body>
<script>
  var targetOP = "https://server.example.com:443";

  window.addEventListener("message", receiveMessage, false);

  function startChecking() {
    checkStatus();
    // Check status every 60 seconds
    setInterval("checkStatus()", 1000*60);
  }

  function getCookieValue(cookieName) {
    var name = cookieName + "=";
    var cookies = document.cookie.split(';');
    if (!cookies) {
      return null;
    }
    for (var i = 0; i < cookies.length; i++) {
      var cookie = cookies[i].trim();
      if (cookie.indexOf(name) == 0) {
        return cookie.substring(name.length, cookie.length);
      }
    }
    return null;
  }

  function checkStatus() {
    var client = "client01";
    var sessionState = getCookieValue("session_state");
    var text = client + " " + sessionState;
    var iframe = document.getElementById("iframeOP");
    iframe.contentWindow.postMessage(text, targetOP);
  }

  function receiveMessage(event) {
    if (event.origin !== targetOP) {
      // Origin did not come from the OP; this message must be rejected
    }
  }
</script>
</body>
</html>
```

```

        return;
    }
    if (event.data === "unchanged") {
        // User is still logged in to the OP
    } else {
        // User has logged out of the OP
    }
}
</script>
</html>

```

## Authentication Filters



8.5.5.5

You can use the authentication filter to determine whether certain HTTP servlet requests are processed by certain providers.

Liberty server authentication filter uses the filter criteria that are specified in the `authFilter` element in the `server.xml` file to determine whether certain HTTP servlet requests are processed by certain providers, such as OpenID, OpenID Connect, or SPNEGO, for authentication.

If all conditions in the `authFilter` element are met, the HTTP servlet request is processed by the particular provider that references that `authFilter` element. If any of the conditions within the `authFilter` element are not met, the HTTP servlet request is not processed by the provider.

### Supported elements

The `authFilter` element supports the following elements: `userAgent`, `host`, `webApp`, `remoteAddress`, and `requestUrl`.

- The `userAgent` element is compared against a corresponding header value that is extracted from the incoming HTTP servlet request. The `userAgent` element is compared against the “User-Agent” HTTP request header, which identifies the client software that is used by the originating request. For web client browsers, this value reflects the browser type that is used to initiate the request (Internet Explorer, Firefox, Safari, etc.).
- The `host` element is used similarly to the `userAgent` element. The `host` element is compared against the “Host” HTTP request header, which identifies the target host name of the request.
- The `webApp` element is used to specify the application, or list of applications, hosted on the Liberty server that is protected by this authentication filter.
- The `remoteAddress` element is compared against the remote TCP/IP address of the client application that sent the HTTP request. You can configure wildcards for specifying subnets and ranges by using the `lessThan` or `greaterThan` values of the `matchType` attribute, as shown among the examples that follow later in this topic.
- The `requestUrl` element is compared against the URL that is used by the client application to make the request. Single URL patterns are configured or piped lists of values are configured, as shown among the examples that follow later in this topic.

### Authentication Filter examples

#### Request URL contains a pattern

The following example shows a typical configuration for an authentication filter. Here, any incoming request with a request URL containing `/SimpleServlet` is processed by the service that is configured to use this filter.

```

<authFilter id="myAuthFilter">
    <requestUrl id="myRequestUrl" urlPattern="/SimpleServlet" matchType="contains"/>
</authFilter>

```

### Request URL contains one of a set of patterns

In the following example, a piped list of request URL patterns is specified. To process an incoming request with the service configured to use this filter, the incoming request URL must contain any one of "/SimpleServlet", "/EmployeeRoleServlet", or "/AllRoleServlet".

```
<authFilter id="myAuthFilter">
    <requestUrl id="myURL" urlPattern="/SimpleServlet|/EmployeeRoleServlet|/AllRoleServlet" matchType="contains"/>
</authFilter>
```

### Web application name contains a pattern

In the following example, a web application name is specified in the authentication filter. Incoming requests must target the "myApp" application to be processed by the service that is configured to use this filter.

```
<authFilter id="myAuthFilter">
    <webApp id="myWebApp" name="myApp" matchType="contains"/>
</authFilter>
```

### Web application name contains one of a set of patterns

In the following example, a piped list of web applications is specified. To process an incoming request with the service configured to use this filter, the incoming request must target any one of the "myApp1", "myApp2", or "myApp3" applications.

```
<authFilter id="myAuthFilter">
    <webApp id="myWebApp" name="myApp1|myApp2|myApp3" matchType="contains"/>
</authFilter>
```

### Request originates from a certain IP address

The following example shows how to use wildcards in the `remoteAddress` element. With this configuration, the service that is configured to use this filter processes the incoming request if the request comes from an IP address anywhere in the 127.0.0.\* range.

```
<authFilter id="myAuthFilter">
    <remoteAddress id="myRemoteAddress" ip="127.0.0.*" matchType="equals"/>
</authFilter>
```

### Excluding patterns

The following example shows how to use a piped list of values for the `requestUrl` element. Matching any of the patterns in the list is sufficient to satisfy the requirements of that particular element. In this example, the request URL must contain either "/SimpleServlet", "/EmployeeRoleServlet", or "/AllRoleServlet". In addition, the request URL must not contain "/ManagerRoleServlet" and the request must come from an Internet Explorer user agent.

```
<authFilter id="myAuthFilter">
    <requestUrl id="myURL1" urlPattern="/SimpleServlet|/EmployeeRoleServlet|/AllRoleServlet" matchType="contains"/>
    <requestUrl id="myURL2" urlPattern="/ManagerRoleServlet" matchType="notContains" />
    <userAgent id="myAgent" agent="IE" matchType="contains" />
</authFilter>
```

### Example using all sub-elements

To process an incoming request with the service configured to use this filter, the request must meet the following conditions:

- Contains the pattern "/SimpleServlet" in the request URL
- Targets a domain that contains "host.example.com"
- Comes from the IP address 127.0.0.1
- Comes from a Firefox browser
- The name of the target application is myApp

```
<authFilter id="myAuthFilter">
    <requestUrl id="myRequestUrl" urlPattern="/SimpleServlet" matchType="contains"/>
    <host id="myHost" name="host.example.com" matchType="contains"/>
    <remoteAddress id="myAddress" ip="127.0.0.1" matchType="equals" />
    <userAgent id="myUserAgent" agent="Firefox" matchType="equals"/>
    <webApp id="myWebApp" name="myApp" matchType="contains"/>
</authFilter>
```

---

## Authorizing access to resources in Liberty

The purpose of authorization is to determine whether a user or group has the necessary privileges to access a resource.

### About this task

To learn about how authorization works in Liberty, see “Liberty: Authorization” on page 999.

The following topics are covered in this section:

### Procedure

- Configure authorization for applications in a Liberty server
- **z/OS** Configure security authorization for users on z/OS(r)

## Configuring authorization for applications in Liberty

Configuring authorization for your application is to verify whether a user or group belongs to a specified role, and whether this role has the privilege to access a resource.

### About this task

The Liberty server extracts user and group mapping information from a user registry, then checks the authorization configuration for the application to determine whether a user or group is assigned to one of the required roles. Then the server reads the deployment descriptor of the application, to determine whether the user or group has the privilege to access the resource.

**z/OS** When using System Authorization Facility (SAF) authorization, roles are mapped to EJBROLE resource profiles using the SAF role mapper. The server queries SAF to determine if the user has the required READ access to the EJBROLE resource profile.

### Procedure

1. Enable the `appSecurity-2.0` Liberty feature in the `server.xml` file.

For example:

```
<featureManager>
  <feature>appSecurity-2.0</feature>
</featureManager>
```

**Note:** **z/OS**

- If you are using the SAF authorization provider, include the `zosSecurity-1.0` feature and define a `safAuthorization` configuration element in your `server.xml` file. For example:

```
<featureManager>
  <feature>appSecurity-2.0</feature>
  <feature>zosSecurity-1.0</feature>
</featureManager>
```

```
<safAuthorization id="saf" />
```

2. Configure a user registry for authentication on the Liberty server.  
See “Authenticating users in Liberty” on page 1850.

**z/OS** If you are using the SAF authorization provider, you must use the SAF registry and the server must be authorized to use SAF authorized services. See “Activating and configuring the SAF registry on z/OS” on page 1857.

3. Ensure that the deployment descriptor for your application includes security constraints and other security related information.

**Note:** You can also use a tool such as Rational Application Developer to create the deployment descriptor.

4. Configure the authorization information such as the user and group to role mapping.

You can configure the authorization table in the following ways:

- If you have an EAR file, you can add the authorization configuration definition to the `ibm-application-bnd.xml` or `ibm-application-bnd.xmi` file.
- If you have standalone WAR files, you can add the authorization table definitions to the `server.xml` file under the respective application element. You can use the WebSphere Application Server Developer Tools for Eclipse to do this.

**Notes:**

- If you have an EAR file, the authorization configuration might already exist. In EAR files that are written to the current specification, this information is stored in an `ibm-application-bnd.xml` file; in older EAR files, this information is stored in an `ibm-application-bnd.xmi` file.
- If your EAR file does not already contain an `ibm-application-bnd.xml` file, it is not a straightforward task to create one and you might prefer to add the authorization configuration to the `server.xml` file.
- If the authorization configuration for the EAR file is defined in an `ibm-application-bnd.xml` file and also in the `server.xml` file, then the two tables are merged. If there are any conflicts, the information from the `server.xml` file is used.
- If you modify your user registry, be sure to review the authorization table for necessary changes. For example, if you are specifying an `access-id` element and change the realm name of the registry, you must also change the realm name in the `access-id` element.
- If you specify the `application-bnd` element in the `server.xml` file, your application must not be in the `dropins` folder. If you leave it in the `dropins` folder, then you must disable application monitoring by setting the following in your `server.xml` file:

```
<applicationMonitor dropinsEnabled="false" />
```

A role can be mapped to a user, a group, or a special subject. The two types of special subject are `EVERYONE` and `ALL_AUTHENTICATED_USERS`. When a role is mapped to the `EVERYONE` special subject, there is no security because everyone is allowed access and you are not prompted to enter credentials. When a role is mapped to the `ALL_AUTHENTICATED_USERS` special subject, then any user who has been authenticated by the application server can access the protected resource.

Here is example code for configuring the user and group to role mapping in the `server.xml` file:

```
<application type="war" id="myapp" name="myapp" location="${server.config.dir}/apps/myapp.war">
  <application-bnd>
    <security-role name="user">
      <group name="students" />
    </security-role>
    <security-role name="admin">
      <user name="gjones" />
      <group name="administrators" />
    </security-role>
    <security-role name="AllAuthenticated">
      <special-subject type="ALL_AUTHENTICATED_USERS" />
    </security-role>
  </application-bnd>
</application>
```

In this example, the **admin** role is mapped to the user ID `gjones` and all users in the group `administrators`. The **AllAuthenticatedRole** is mapped to the special subject `ALL_AUTHENTICATED_USERS`, meaning that any user has access as long as they provide valid credentials for authentication.

**z/OS** If you are using SAF authorization, roles are mapped to EJBROLE resource profiles using the SAF role mapper. The SAF role mapper pattern can be configured using the **safRoleMapper**

element in the `server.xml` file. See “Liberty: Controlling how roles are mapped to SAF Profiles.” By default, the role is mapped to a resource profile using the pattern `profile_prefix.resource.role`, where

- `profile_prefix` is defined by the `profilePrefix` attribute on the `safCredentials` configuration element. By default, the value of `profilePrefix` is `BBGZDFLT`.
- `resource` is the resource name; for example, the application name.
- `role` is the role name.

To access the protected resource, the user must have `READ` access to the `EJBROLE` resource profile. For example, for user ID `gjones` to access a protected resource under the role `admin` for the application `myapp`, the user `gjones` must have `READ` access to the resource profile `BBGZDFLT.myapp.admin` in the `EJBROLE` class in the SAF product.

**Note:** `EJBROLE` resource profiles are case sensitive.

The following example code shows sample RACF commands for authorizing a user:

```
rdef EJBROLE BBGZDFLT.myapp.admin uacc(none)
permit BBGZDFLT.myapp.admin class(EJBROLE) access(read) id(gjones)
```

## Liberty: Controlling how roles are mapped to SAF Profiles

z/OS

The System Authorization Facility (SAF) role mapper determines how `EJBROLE` profile names are generated from application-defined role names. The mapper is invoked whenever SAF authorization is performed for an application role. The authorization check for the application role is made against the underlying SAF security product using the mapped profile name generated by the SAF role mapper.

The SAF role mapper can be configured by using the `<safRoleMapper>` configuration element.

```
<safRoleMapper profilePattern="myprofile.%.resource%.role%" toUpperCase="true" />
```

### Attributes

#### `profilePattern="<string>"`

The pattern used to map application roles to profile names.

- `%role%` is substituted at run time with the value of the application role
- `%resource%` is substituted with the resource name. For example, the application name.

For example, for `profilePattern="myprofile.%.resource%.role%"`, the profile generated for an access check to the resource `"myapp"` for the `"admin"` role, is `myprofile.myapp.admin`.

The list of supported substitution variables:

#### `%role%`

The application role name. For the administrator role, the value is `Administrator`.

#### `%resource%`

The protected resource name. For security administration, the resource name is `com.ibm.ws.management.security.resource`.

#### `%profilePrefix%`

The `profilePrefix`, defined by the `profilePrefix` attribute in the `<safCredentials>` config element. The default value is `BBGZDFLT`.

If not specified, the default is `profilePattern="%.profilePrefix%.resource%.role%"`

#### `toUpperCase="true|false"`

Indicates whether the mapped profile name should be folded to uppercase.

If not specified, the default is `false`.

**Note:** The SAF role mapper will automatically substitute any wildcard characters (%&\*) and whitespaces in the mapped profile name with the '#' character.

## Enabling z/OS authorized services in Liberty for z/OS

z/OS

Liberty on z/OS offers the ability for your applications to take advantage of z/OS authorized services for System Authorization Facility (SAF) authorization, Workload Manager (WLM), Resource Recovery services (RRS), and SVCDUMP. If your application requires these services, set up a Liberty angel process and grant access for your Liberty server to use these services.

### About this task

To use the z/OS Authorized Services, you can set up the following types of profiles by using a SAF security product such as RACF:

- SAF STARTED profile is required if you plan on running the Liberty server or the Liberty angel process as a z/OS Started Task. For more information about the Liberty angel process, see “Liberty profile: Process types on z/OS” on page 1019.
- SAF SERVER profile is required if you plan on having the Liberty server access any of the z/OS Authorized Services for your applications. You can find the description of each service in the following content.

**Note:** You do not need to set up RACF if you are not planning to run the Liberty server as a Started Task and you are not planning to use any of the authorized services.

### Procedure

- Create STARTED profiles for the PROCs for the angel and Liberty server processes. This action enables the angel and Liberty server to run as Started Tasks.

- To cause the angel to run under the user ID *WLPUSER0*:

```
rdef started bbgzangl.* uacc(none) stdata(user(WLPUSER0) group(wasuser) privileged(no) trusted(no) trace(yes))
```

- To cause a server that is running under the BBGZSRV procedure name to run under the user ID *WLPUSER1*:

```
rdef started bbgzsrv.* uacc(none) stdata(user(WLPUSER1) group(wasuser) privileged(no) trusted(no) trace(yes))
```

- Create a SERVER profile for the angel process and permit the *WLPUSER1* user ID. This action grants a Liberty server access to the angel process, which is required for the z/OS authorized services. To enable a server that is running as *WLPUSER1* to connect to the angel:

```
RDEF SERVER BBG.ANGEL UACC(NONE)  
PERMIT BBG.ANGEL CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

- Create a SERVER profile for the authorized module BBGZSAFM and permit the Started Task user ID of the Liberty server to the profile. This action enables a Liberty server to use the z/OS Authorized services. To enable a server that is running as *WLPUSER1* to access the authorized module:

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM UACC(NONE)  
PERMIT BBG.AUTHMOD.BBGZSAFM CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

- Create SERVER profiles for the individual authorized services provided for the z/OS platform. These profiles enable the server to invoke the individual authorized services and these services are grouped by function:

- To enable the SAF authorized user registry services and SAF authorization services (SAFCRED):

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.SAFCRED UACC(NONE)  
PERMIT BBG.AUTHMOD.BBGZSAFM.SAFCRED CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

- To enable the WLM services (ZOSWLM):

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.ZOSWLM UACC(NONE)  
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSWLM CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

- To enable the RRS transaction services (TXRRS):

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.TXRRS UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.TXRRS CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

- To enable the SVCDUMP services (ZOSDUMP):

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.ZOSDUMP UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSDUMP CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

-  **8.5.5.2** To enable optimized local adapter services:

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.LOCALCOM UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.LOCALCOM CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.WOLA UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.WOLA CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

- **8.5.5.2** To enable the IFAUSAGE services (PRODMGR):

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.PRODMGR UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.PRODMGR CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

- To enable the AsyncIO services (ZOSAIO):

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.ZOSAIO UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSAIO CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

-  **8.5.5.2** Create a SERVER profile for the authorized client module BBGZSCFM and permit the Started Task user ID of the Liberty server to the profile. This action enables a Liberty server to load the z/OS Authorized client services. To enable a server that is running as WLPUSER1 to access the authorized client module:

```
RDEF SERVER BBG.AUTHMOD.BBGZSCFM UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSCFM CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

-  **8.5.5.2** Create SERVER profiles for the individual authorized client services provided for the z/OS platform. These profiles enable clients to invoke the individual authorized services provided by the server. These services are grouped by function:

- To enable optimized local adapter services:

```
RDEF SERVER BBG.AUTHMOD.BBGZSCFM.WOLA UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSCFM.WOLA CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

## Liberty: Accessing z/OS security resources using WZSSAD

z/OS

The WebSphere Liberty z/OS System Security Access Domain (WZSSAD) refers to the permissions granted to the Liberty server. These permissions control which System Authorization Facility (SAF) application domains and resource profiles the server is permitted to query when authenticating and authorizing users.

For example, if you want to set up two Liberty server instances, one for production and one for test and you want your role access to be different between production and test, you can set up two different System Security Access Domains.

The Liberty server is an unauthorized program that can be configured and run by non-administrator or non-privileged users, so it is important for system security and integrity purposes that the user is prevented from leveraging the server to run security operations for which they have not been explicitly granted permission.

**Note:** The WZSSAD is in effect only when the server is using authorized SAF services for authentication and authorization. This means the angel process is running, and the server has been granted permission to use the SAFCREED authorized service routines.

There are three SAF operations that are protected by the WZSSAD:

- Authenticating a user

- Authorizing a Subject to a Java EE role
- Authorizing a Subject to other SAF resources

By default, the WZSSAD is not configured, which means the server has no permission to authenticate or authorize anything. For example, the Liberty server cannot use authorized SAF services for authentication or authorization until an administrator grants it permission to perform some or all of the operations.

## Authenticating a user

The server authenticates users to a particular SAF domain that is configured by defining a resource, which is referred to as the APPLID in the APPL class. In order to authenticate a user to the domain, the user must have READ access to the APPLID resource in the APPL class. In addition, whenever the APPL class is active, the unauthenticated user ID (which is WSGUEST by default) also requires READ access to the APPLID resource in the APPL class.

The APPLID resource name used by the server is specified by the **profilePrefix** attribute in the <saxCredentials> configuration element. If you do not specify this element, then the default profilePrefix of BBGZDFLT is used.

The following example shows how to configure a **profilePrefix** of BBGZDFLT in the server.xml file:

```
<saxCredentials profilePrefix="BBGZDFLT"/>
```

The following example shows how to use RACF commands to configure the APPLID as BBGZDFLT:

```
// Define the BBGZDFLT APPLID to RACF.
RDEFINE APPL BBGZDFLT UACC(NONE)

// Activate the APPL class.
//If not active, the domain is not restricted, which means anyone can authenticate to it.
SETROPTS CLASSACT(APPL)

//All users to be authenticated by the server must have READ access to the APPLID in the APPL class:
PERMIT BBGZDFLT CLASS(APPL) ACCESS(READ) ID(UserID)

//The unauthenticated user ID requires READ access to the APPLID in the APPL class:
PERMIT BBGZDFLT CLASS(APPL) ACCESS(READ) ID(WSGUEST)
```

In addition, the server must be granted permission within the WZSSAD to make authentication calls in the given APPLID domain. This prevents an unauthorized user from leveraging the server's use of authorized SAF services to discover information about which APPLIDs can and cannot be authenticated. To grant the server permission to authenticate in a particular APPLID domain, the started task ID of the Liberty server must be granted READ access to the BBG.SECPFX.<APPLID> profile in the SERVER class:

```
RDEFINE SERVER BBG.SECPFX.BBGZDFLT UACC(NONE)
PERMIT BBG.SECPFX.BBGZDFLT CLASS(SERVER) ACCESS(READ) ID(serverUserId)
```

## Authorizing a Subject to a Java EE role

The server authorizes a subject against a Java EE application security role name by checking whether the subject is authorized to a SAF resource profile defined in the EJBROLE class. The SAF resource profile name is mapped from the application role name via the SAF role mapper. The SAF role mapper generates a SAF profile name for a given application role name and application resource name. By default, it generates the SAF profile name using the pattern *{profilePrefix}.{resource}.{role}*. For example:

```
profilePrefix="BBGZDFLT"
```

```
Application resource name = "MYAPP"
```

Application role name = "ADMIN"

Mapped profile name = "BBGZDFLT.MYAPP.ADMIN"

For more information, see “Liberty: Controlling how roles are mapped to SAF Profiles” on page 1941

The WZSSAD restricts which SAF profiles in the EJBROLE class the server is allowed to perform authorization against. This prevents an unauthorized user from leveraging the server's use of authorized SAF services to discover information about which EJBROLE profiles can or cannot be authorized to. The server must be granted permission to run authorization checks against the HLQ of the EJBROLE profile name. The HLQ of the profile name is the first segment of the profile name, up to but not including the first '.'. For example:

EJBROLE profile name = "BBGZDFLT.ADMIN"

HLQ = "BBGZDFLT"

To grant the server permission to run authorization checks against the profile HLQ, the user associated with the server process must be granted READ access to the BBG.SECPFX.<HLQ> profile in the SERVER class:

```
RDEFINE SERVER BBG.SECPFX.BBGZDFLT UACC(NONE)
PERMIT BBG.SECPFX.BBGZDFLT CLASS(SERVER) ACCESS(READ) ID(serverUserId)
```

In the example, because the SAF role mapper sets the HLQ of the mapped profile to the profilePrefix, the same profile BBG.SECPFX.BBGZDFLT governs both the APPLID authentication permissions, and the EJBROLE profile authorization permissions.

## Authorizing a Subject to other SAF resources

Java EE applications can perform access control checks against SAF classes other than EJBROLE. The WZSSAD restricts which SAF classes outside of EJBROLE the server is allowed to authorize against. This prevents an unauthorized user or application from leveraging the server's use of authorized SAF services to discover information about which resource profiles in non-EJBROLE SAF classes the user or application is or is not authorized to.

To grant the server permission to perform authorization checks against non-EJBROLE SAF classes, the user associated with the server process must be granted READ access to the BBG.SECCLASS.<SAF-CLASS> profile in the SERVER class. For example, to authorize against a profile in the FACILITY class:

```
RDEFINE SERVER BBG.SECCLASS.FACILITY UACC(NONE)
PERMIT BBG.SECCLASS.FACILITY CLASS(SERVER) ACCESS(READ) ID(serverUserId)
```

**Note:** There are no restrictions on which resource profiles within the non-EJBROLE class the server is allowed to authorize against. If the server has been granted permission to perform authorization checks against a non-EJBROLE class, then it can authorize against any profile in that class.

## Enabling Asynchronous TCP/IP sockets I/O for Liberty on z/OS

z/OS

You can use the Asynchronous TCP/IP sockets I/O for Liberty (AsyncIO) on z/OS service to provide the basic capabilities of an Asynchronous I/O package at the operating system level. The AsyncIO on z/OS service uses native services to provide improvements in performance and scalability in many environments.

### About this task

To enable the AsyncIO on z/OS service, you define the security setup to permit the Authorized AsyncIO Service(ZOSAIO):

## Procedure

- Start the Angel process:

```
START bbgzangl
```

For more information, see [Administering Liberty on z/OS](#).

- Define the security setup to permit the Authorized AsyncIO Service(ZOSAIO):

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.ZOSAIO UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSAIO CLASS(SERVER) ACCESS(READ) id(wlpuser1)
```

For more information, see [Enabling z/OS authorized services in Liberty for z/OS](#).

## What to do next

This procedure enables the AsyncIO on z/OS service by default. However, if the AsyncIO z/OS service is enabled, you can disable it within a particular server by adding the following to the `server.xml`:

```
<zosaio id="defaultZOSAIO" zosaio.enable="false"/>
```

You must then restart the server to override the default behavior.

## Liberty: Unauthorized services used by the SAF registry

z/OS

The System Authorization Facility (SAF) registry uses a number of unauthorized services from the C environment provided by LE (Language Environment<sup>®</sup>).

The following table lists the unauthorized services from LE C that the SAF registry uses, and provides links to additional information in the z/OS V2R1 information center. These services are subject to BPX.DAEMON restrictions which are detailed in the documentation linked to from the service calls associated with each method listed in the table.

Method	Link to further information
<code>checkPassword(String, String)</code> <code>__passwd_applid()</code>	Verify/Change User Password
<code>getGroups(String, int)</code> <code>setgrent()</code>	Reset Group Database to First Entry
<code>getgrent()</code>	Get Group Database Entry
<code>endgrent()</code>	Get Group Database Entry Functions
<code>getGroupsForUser(String)</code>	Get Supplementary Group IDs by User Name
NOTE: This method only works for users with defined OMVS segments.	
<code>getgroupsbyname()</code>	Get Supplementary Group IDs by User Name
<code>getgrgid()</code>	Access the Group Database by ID
<code>getUsers(String, int)</code> <code>setpwent()</code>	Reset User Database Search
<code>getpwent()</code>	Get User Database Entry
<code>endpwent()</code>	User Database Functions
<code>isValidGroup(String)</code> <code>getgrnam_r()</code>	Search Group Database for a Name
<code>isValidUser(String)</code> <code>getpwnam_r()</code>	Search User Database for a Name

Method	Link to further information
mapCertificate(X509Certificate) __certificate()	Register/Deregister/Authenticate a Digital Certificate

**Note:** If the Liberty server is configured to use SAF authorized services (see “Activating and configuring the SAF registry on z/OS” on page 1857), then the following unauthorized services are not used:

- checkPassword: \_\_passwd\_applid
- isValidUser: getpwnam\_r
- mapCertificate: \_\_certificate

Instead, the Liberty server will use the authorized SAF service initACEE.

## Liberty: Setting up the System Authorization Facility (SAF) unauthenticated user

z/OS

If you are using a SAF user registry, it is necessary to specify a SAF user ID that represents the unauthenticated state. The name of the unauthenticated user ID is specified on the `unauthenticatedUser` attribute of the `SAFCredentials` element in `server.xml`. It is important to define this user ID correctly in your SAF registry. If you are using a RACF SAF user registry, the unauthenticated user (default WSGUEST) needs a unique default group (DFLTGRP) with no other user IDs connected to that group, an OMVS segment, but not a TSO segment, and the options NOPASSWORD, NOOIDCARD, and RESTRICTED. If you have another SAF user registry, instead of RACF, then find the user ID options that are provided by that SAF registry that are equivalent to these RACF options.

### About this task

By running the appropriate commands, you can correctly set up an unauthenticated user in your SAF user registry. An unauthenticated user that is incorrectly setup might cause a security exposure.

### Procedure

1. Run the **ADDGROUP** command. Use WSGUESTG as the group name.

```
ADDGROUP WSGUESTG SUPGROUP(SYS1)OWNER(SYS1)
        DATA('WAS Unauthenticated User Group')
        OMVS(AUTOGID)
```

2. Run the **ADDUSER** command. Use WSGUEST as the user ID name.

```
ADDUSER WSGUEST DFLTGRP(WSGUESTG) OWNER(SYS1)
        OMVS(AUTOUID)
        HOME(/u/WSGUEST)
        PROGRAM(/bin/sh)
        NAME('WAS unauth')
        NOPASSWORD NOOIDCARD
        RESTRICTED
```

The options NOPASSWORD and NOOIDCARD protect this user ID from being revoked by repeated attempts to guess the password.

The option RESTRICTED means that this user ID cannot gain access to protected resources unless it is explicitly permitted to that resource, even is that resource has a general access setting of UACC(READ).

- 3.

**Note:** After the unauthenticated user ID (WSGUEST) is defined to the SAF registry, ensure that the user ID is permitted to only the minimum number of SAF resources. If the Liberty server is using SAF APPL resource check to control which users can connect to the Liberty z/OS System Security Access Domain, then the unauthenticated user ID must be given access to the APPL profile. Run the **PERMIT** command.

```
PERMIT BBGZDFLT CLASS(APPL) ID(WSGUEST) ACCESS(READ)
```

## What to do next

If you receive the RACF authorization failure message ICH408I because the unauthenticated user (WSGUEST) does not have access to a RACF resource, such as an EJBROLE profile. It is nearly always incorrect to permit the unauthenticated user ID to the resource profile to resolve the problem. It usually means that the request is running in an unauthenticated state when it should be running in an authenticated state. The actual problem is probably a failure to authenticate properly. Whenever it appears necessary to permit the unauthenticated user ID to a SAF resource profile you should consider carefully whether that is the correct action to take. Permitting the unauthenticated user ID to any SAF resource profile makes that resource available to everyone, including users that are not authenticated. There are almost no instances where that is required, however, the APPL profile that controls access to the WZSSAD is one exception.

## Configuring distributed identity filters in z/OS security

z/OS

Distributed identity filters must be configured when the `mapDistributedIdentities` attribute in the `safCredentials` configurations element is set to true.

### About this task

Before you map distributed identities to System Authorization Facility (SAF) users, you must first configure distributed identity filters in z/OS security.

The distributed identity filter in the SAF class RACMAP consists of the distributed user name and the realm name of the distributed user name. You can configure the filters to map many distributed identities to one SAF user or you can have a one-to-one mapping.

The following example illustrates the syntax for creating a distributed identity filter that uses the RACMAP command:

```
RACMAP ID(<SAFUser>) MAP USERDIDFILTER(NAME('<distributedUserId>'))
REGISTRY(NAME('<distributedRealmName>'))
    WITHLABEL('<someLabel>')
```

In the example:

- The *SAFUser* element is the SAF user in z/OS security.
- The *distributedUserID* element is the distributed identity.
- The *distributedRealmName* element is the realm name of the distributed identity.
- The *someLabel* element is a field that describes this distributed identity filter.

### Procedure

1. Activate the IDIDMAP class. This command needs to be run only once at the beginning. SETROPTS CLASSACT(IDIDMAP) RACLIST(IDIDMAP)
2. After you edit the RACMAP profiles, you must use the following command for the changes to take effect: SETROPTS RACLIST(IDIDMAP) REFRESH

### Example

The following example illustrates the LDAP user (LDAPUser1) mapped to the SAF user (USER1):

```
RACMAP ID(USER1) MAP USERDIDFILTER(NAME('CN=LDAPUser1,o=ibm,c=us'))
REGISTRY(NAME('ccwin12.austin.ibm.com:389'))
WITHLABEL('Mapping LDAP LDAPUser1 to USER1')
```

## Securing optimized local adapters on Liberty for z/OS

z/OS



8.5.5.2

In addition to configuring security on your Liberty server, you can further secure WebSphere optimized local adapters (WOLA) connections with the System Authorization Facility (SAF) CBIND class, security parameters on the optimized local adapter APIs, and more.

## Securing optimized local adapters for inbound support in Liberty for z/OS

z/OS



8.5.5.2

Secure your WebSphere optimized local adapters (WOLA) connections that make inbound calls to the Liberty server.

### Before you begin

Run the Liberty servers on z/OS with server security. For more information, see “Liberty: Security” on page 971.

Local access to Liberty for z/OS servers is protected by the System Authorization Facility (SAF) CBIND class. When enabled, this class is used to protect Liberty servers when optimized local adapters requests are made. Before you run any application that uses the Register API, grant READ access for the user ID for the job, UNIX System Services process, or Customer Information Control System (CICS) region to the CBIND class for the target server.

All inbound requests to the Liberty server run under the authority of the current user on thread. This identity is automatically propagated and asserted in the Enterprise JavaBeans (EJB) container, and the application starts under this identity. Inbound requests that drive into a target enterprise bean arrive in the same manner as method invocations do for local EJB requests, and the security options for RunAs work in the same way as local EJB requests.

When inbound or outbound transaction work passes between CICS and Liberty for z/OS, you must take into account some special security considerations. For example, you must determine if the authentication for inbound to the Liberty server work should run with the authority of the specific CICS application or the overall CICS region authority. There are similar concerns when the Liberty server sends outbound work to a CICS application; you must determine if CICS should honor the originating application authority or its own CICS current security profile.

**Attention:** You must make sure that the client applications are authenticated for CICS to process the request.

For passing requests in to the Liberty server from CICS, you can indicate that you want to use the current CICS application identity by setting a flag for this with the Register API call.

### Procedure

- Create SERVER profiles for z/OS.
  1. Create SERVER profiles for the optimized local adapter authorized service. Use the following Time Sharing Option (TSO) commands:

```
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.LOCALCOM UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.LOCALCOM CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
RDEF SERVER BBG.AUTHMOD.BBGZSAFM.WOLA UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.WOLA CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

2. Create a SERVER profile for the authorized client module BBGZSCFM and permit the Started Task user ID of the Liberty server to the profile. This action enables a Liberty server to load the z/OS Authorized client services. To enable a server that is running as WLPUSER1 to access the authorized client module:

```
RDEF SERVER BBG.AUTHMOD.BBGZSCFM UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSCFM CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

3. Create SERVER profiles for optimized local adapter authorized client service. Use the following TSO commands:

```
RDEF SERVER BBG.AUTHMOD.BBGZSCFM.WOLA UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSCFM.WOLA CLASS(SERVER) ACCESS(READ) ID(WLPUSER1)
```

For more information, see “Enabling z/OS authorized services in Liberty for z/OS” on page 1942.

- If you have CBIND enabled in System Authorization Facility (SAF), grant access to the clients that will use optimized local adapters.

1. Define a profile for the Liberty server in the CBIND class. The profile name is BBG.WOLA.<WOLA1>.<WOLA2>.<WOLA3>, where WOLA1,WOLA2, and WOLA3 are the three parts of the optimized adapter group name that are specified in the <zosLocalAdapters> element in the server.xml file. You can define a profile by using the SAF **RDEFINE** TSO command. For example, the following command creates a profile in the CBIND class for a WOLA group named LIB1.LIB2.LIB3:

```
RDEF CBIND BBG.WOLA.LIB1.LIB2.LIB3 UACC(NONE)
```

2. Permit READ access to the profile. For example, the following command permits read access for the *username* user name on the bbg.wola.lib1.lib2.lib3 profile:

```
PERMIT BBG.WOLA.LIB1.LIB2.LIB3 CLASS(CBIND) ACCESS(READ) ID(USERNAME)
```

You can use asterisks to permit a user access to multiple profiles. The following example permits READ access to the *username* user for all profiles that start with bbg.wola in the CBIND class:

```
RDEF CBIND BBG.WOLA.* UACC(NONE)
PERMIT BBG.WOLA.* CLASS(CBIND) ACCESS(READ) ID(USERNAME)
```

For more information about SAF commands and syntax, see the documentation for your version of z/OS.

- Configure the security settings. The security identity propagation type is specified in registration flags when the optimized local adapters connection request is made in the call to the Register API. For more information, see “Optimized local adapters APIs on Liberty for z/OS” on page 2079. You can select either the CICS region or application security profile.

**Attention:** For security propagation to function, you must enable security at the CICS application level by setting the SEC=Y CICS startup option.

## Securing optimized local adapters for outbound support in Liberty for z/OS



Secure your WebSphere optimized local adapters (WOLA) connections that make outbound calls from the Liberty server.

### Procedure

1. Optional: Set up server-side security.
  - a. Run the Liberty servers on z/OS with server security. For more information, see “Configuring authorization for applications in Liberty” on page 1939 and “Enabling z/OS authorized services in Liberty for z/OS” on page 1942.
  - b. If you are calling from a Liberty server to Customer Information Control System (CICS) and security is enabled on the CICS link server, choose a user ID to run the target CICS program.

By default, the invocation subject obtains the MVS user ID that runs the target CICS program. The invocation subject is the subject that runs the application component that makes the optimized local adapters request. In many cases, this subject is the run-as identity that is configured in the application deployment descriptor.

You can define an alternative subject to the invocation subject in three ways:

- In the connection factory configuration, specify a user ID and password in an `authData` element, and reference the element in the `connectionFactory` element. In the following example, the optimized local adapter connection factory references the `auth2` `authData` element, which specifies a user ID of `user2` and an associated password.

```
<connectionFactory jndiName="eis/ola" containerAuthDataRef="auth2">
  <properties.ola RegisterName="OLASERVER"/>
</connectionFactory>
<authData id="auth2" user="user2" password="{xor}Lz4sLCgwLTtt"/>
```

For more information about configuring connection factories, see “Configuring JCA connection factories” on page 1618.

- The system administrator can provide a user ID and password on the optimized local adapters connection factory. For more information, see “Connection factory properties for optimized local adapters on Liberty” on page 1699.
- The application developer can provide a user ID and password on the `ConnectionSpec` object that obtains a connection from the optimized local adapters connection factory.

The security service attempts to authenticate with the provided user ID and password. If authentication is successful, the new subject obtains the MVS user ID that runs the target CICS program.

- c. If you are calling from a Liberty server to IBM Information Management System (IMS) by using OTMA, the Liberty server can propagate the current user ID to the IMS region if the Liberty server and the application are both configured to use `sync-to-OS-thread`. The IMS region must also be running with the option `OTMASE=FULL` in the `IMSPBxxx PROCLIB` member.
2. Set up client-side security.
    - a. If you have `CBIND` enabled in System Authorization Facility (SAF), grant access to the clients that will use optimized local adapters.
      - 1) Define a profile for the Liberty server in the `CBIND` class. The profile name is `BBG.WOLA.<WOLA1>.<WOLA2>.<WOLA3>`, where `WOLA1`, `WOLA2`, and `WOLA3` are the three parts of the optimized adapter group name that are specified in the `<zosLocalAdapters>` element in the `server.xml` file. You can define a profile by using the SAF **RDEFINE** TSO command. For example, the following command creates a profile in the `CBIND` class for a `WOLA` group that is named `LIB1.LIB2.LIB3`:
 

```
rdef cbind bbg.wola.lib1.lib2.lib3 uacc(none)
```
      - 2) Permit `READ` access to the profile. For example, the following command permits read access for the `username` user name on the `bbg.wola.lib1.lib2.lib3` profile:
 

```
permit bbg.wola.lib1.lib2.lib3 class(cbind) access(read) id(username)
```

You can use asterisks to permit a user access to multiple profiles. The following example permits `READ` access to the `username` user for all profiles that start with `bbg.wola` in the `CBIND` class:

```
rdef cbind bbg.wola.* uacc(none)
permit bbg.wola.* class(cbind) access(read) id(username)
```
- For more information about SAF commands and syntax, see the documentation for your version of z/OS.
- b. If you are running a CICS link server with security enabled, configure CICS to enable user identity assertion.
    - 1) Ensure that the CICS region is running with security enabled and `EXEC CICS START` checking enabled.
      - Enable security at CICS startup by specifying the parameter `SEC=YES`.

- Enable EXEC CICS START checking at startup by specifying the parameter XUSER=YES.

For more information about CICS system initialization parameters, see the documentation for your version of CICS.

- 2) Create a System Authorization Facility (SAF) SURROGAT class definition that permits the user ID of the link server to issue the EXEC CICS START TRAN('BBO#') USERID(<propagated\_id>) command.

The following example shows a SURROGAT class that is defined for the USER1 user ID. The class enables user ID OLASERVE to run the EXEC CICS START TRANS(BBO#) USERID(USER1) command and process optimized local adapters CICS link transactions that run with the identity of USER1.

```
RDEFINE SURROGAT USER1.DFHSTART UACC(NONE) OWNER(USER1)
PERMIT USER1.DFHSTART CLASS(SURROGAT) ID(USER1)
PERMIT USER1.DFHSTART CLASS(SURROGAT) ID(OLASERVE)
SETROPTS RACLIST(SURROGAT) REFRESH
```

For more information about defining a SURROGAT class, see the documentation for your version of CICS.

## Configuring security authorization for Liberty servers on IBM i

IBM i

Using the iAdmin GRANTAUTH command, you can authorize the QEJBSVR user profile to access the required resources for running the Liberty server.

### Before you begin

Servers run under the QEJBSVR user profile if one of the following is true:

- The Liberty environment was installed as a feature of a product offering using the IBM Installation Manager.
- The iAdmin POSTINSTALL command was called after Installing Liberty by extracting an archive file.

Also, QEJBSVR is granted authorization to files in the \$WLP\_USER\_DIR and \$WLP\_OUTPUT\_DIR locations in all of these installation scenarios. Additionally, when servers are created, QEJBSVR is granted authorization to server definition files and the \$WLP\_OUTPUT\_DIR location.

### About this task

This task provides example commands that show you how to authorize the QEJBSVR user profile to access the required resources for running the server after doing the following tasks:

- Creating files manually or modifying the authorities on shared resources and server definitions files.
- Configuring a server to access resources the QEJBSVR user profile is not yet authorized to.

### Example

- Granting the server role to the QEJBSVR user profile for the shared resources, server definitions and output locations configured for the Liberty environment installed at /WAS/wlp directory.  

```
/WAS/wlp/lib/native/os400/bin/iAdmin GRANTAUTH -rolename server -userprofilename QEJBSVR
```
- Granting the server role to the QEJBSVR user profile for shared resources and server definitions in /WAS/myWlpServers/usr, and for any server output locations defined by the WLP\_OUTPUT\_DIR variable in files matching the definition in the /WAS/myWlpServers/usr/servers/\*/server.env file.  

```
/WAS/wlp/lib/native/os400/bin/iAdmin GRANTAUTH -rolename server -userprofilename QEJBSVR
-userdir /WAS/myWlpServers/usr
```
- Granting the server role to the QEJBSVR user profile for output location /WAS/myWlpOutput/servers.

```
/WAS/wlp/lib/native/os400/bin/iAdmin GRANTAUTH -rolename server -userprofilename QEJBSVR  
-outputdir /WAS/myWlpOutput/servers
```

## OAuth

8.5.5.0

OAuth is an open standard for delegated authorization. With the OAuth authorization framework, a user can grant a third-party application access to their information stored with another HTTP service without sharing their access permissions or the full extent of their data.

In OAuth, the client, or third-party application, requests access to resources controlled by the resource owner and hosted by the resource server, and is issued a different set of credentials than those of the resource owner. Instead of using the credentials of the resource owner to access protected resources, the client obtains an access token, which is a string denoting a specific scope, lifetime, and other access attributes. Access tokens are issued to third-party clients by an authorization server with the approval of the resource owner. The client uses the access token to access the protected resources hosted by the resource server.

OAuth 2.0 is not compatible with OAuth 1.0. OAuth 2.0 provides ease of use for client application developers, and authorization flows for different types of client applications.

WebSphere Application Server supports OAuth 2.0, and can be used as an OAuth service provider endpoint and an OAuth protected resource enforcement endpoint.

WebSphere Application Server supports the following OAuth standard specifications:

- The OAuth 2.0 Authorization Framework
- The OAuth 2.0 Authorization Framework: Bearer Token Usage

The following list shows a summary of features within WebSphere Application Server OAuth 2.0 services.

- WebSphere Application Server acts as an OAuth Service Provider (SP) to handle OAuth 2.0 protocol requests.
- WebSphere Application Server acts as protected resource enforcement endpoint to authorize or deny requests for deployed web resources.
- Allow multiple service providers to co-exist.
- Allow administrator to revoke access tokens.
- Allow client to revoke its authorization given by a user.
- Optionally provide a Subject for a resource application to make an authenticated downstream call or perform programmatic J2EE security.
- Support 4 typical OAuth 2.0 flows as defined in the protocol.
- Support persistent OAuth services.

### OAuth 2.0 services

8.5.5.0

WebSphere Application Server OAuth services include both the OAuth authorization service and the web resource authorization decision service.

The OAuth 2.0 authorization service provides all OAuth 2.0 protocol endpoint URLs, and is responsible for client authorization and token issuing.

The web resource authorization decision service is built into the Liberty web authentication code. When a client accesses an OAuth protected web resource, the OAuth token is validated and mapped to a WebSphere Application Server platform security subject that the web request then runs under.

## Defining an OAuth service provider: **8.5.5.0**

An OAuth service provider is a named set of configuration options for OAuth. The id or name of the provider is specified in the URL of inbound requests to the authorization and token endpoints. The set of configuration options for that provider is used when the request is handled. This process allows one server with one endpoint servlet to effectively provide multiple OAuth configurations. For example, the `https://my.company.com:8021/oauth2/endpoint/photoShare/authorize` URL is handled by using the set of OAuth configuration options that are defined for the OAuth provider named `photoShare`. The `https://my.company.com:8021/oauth2/endpoint/calendarAuthz/authorize` URL is handled by using the set of OAuth configuration options that are defined for the OAuth provider named `calendarAuthz`.

### About this task

An OAuth service provider is defined with the `oauthProvider` element in the `server.xml` file. You can define an OAuth service provider by editing the `server.xml` file or by using the WebSphere Application Server Development Tools for Liberty. This task describes how to define a minimal OAuth configuration.

### Procedure

1. Add the `oauth-2.0` and `ssl-1.0` features. OAuth is a secure protocol so SSL is required. On Liberty, you must supply a keystore password for SSL by using the `keyStore` element. There is no default keystore password.

```
<featureManager>
  <feature>oauth-2.0</feature>
  <feature>ssl-1.0</feature>
</featureManager>
```

2. Set up the role mapping for the OAuth web application by using the `oauth-roles` element. OAuth is an HTTP-based protocol and a web application is supplied to handle the authorization and token endpoints. The web application is built in and is started automatically when you specify the `oauth-2.0` feature. However, you must map the authenticated role to one or more users, groups, or special subjects. Another role, `clientManager`, is supplied for managing client configuration, but it is not necessary to map that role for OAuth authorization to function.

```
<oauth-roles>
  <authenticated>
    <user>testuser</user>
  </authenticated>
</oauth-roles>
```

3. Define one or more providers with the `oauthProvider` element. The provider must have at least one client defined. Clients can be defined locally with the `localStore` and `client` elements. Clients can also be defined in a relational database with the `databaseStore` element.

```
<oauthProvider id="SampleProvider" filter="request-url%=ssodemo">
  <localStore>
    <client name="client01" secret="{xor}LDo8LTor"
      displayname="Test client number 1"
      redirect="http://localhost:1234/oauthclient/redirect.jsp"
      enabled="true" />
  </localStore>
</oauthProvider>
```

4. **8.5.5.0** Define a user registry, either an LDAP registry by specifying the `ldapRegistry-3.0` feature and the `ldapRegistry` configuration element, or a basic registry by specifying the `basicRegistry` configuration element.

```

<basicRegistry id="basic" realm="BasicRealm">
  <user name="testuser" password="testuserpwd" />
</basicRegistry>

```

5. Set the `allowFailOverToBasicAuth` web application security property to `true`.

```

<webAppSecurity allowFailOverToBasicAuth="true" />

```

## Results

You have defined a minimal OAuth configuration.

## Example

The following example shows a sample `server.xml` file that defines a simple OAuth provider with one client:

```

<server>

  <featureManager>
    <feature>oauth-2.0</feature>
    <feature>ssl-1.0</feature>
  </featureManager>

  <keyStore password="keyspass" />

  <oauth-roles>
    <authenticated>
      <user>testuser</user>
    </authenticated>
  </oauth-roles>

  <oauthProvider id="SampleProvider" filter="request-url%ssodemo">
    <localStore>
      <client name="client01" secret="{xor}LDo8LTor"
        displayname="Test client number 1"
        redirect="http://localhost:1234/oauthclient/redirect.jsp"
        enabled="true" />
    </localStore>
  </oauthProvider>

  <webAppSecurity allowFailOverToBasicAuth="true" />

  <basicRegistry id="basic" realm="BasicRealm">
    <user name="testuser" password="testuserpwd" />
  </basicRegistry>

</server>

```

## OAuth full profile provider configuration equivalents: **8.5.5.0**

The following tables map the Liberty `server.xml` file elements and attributes to the equivalent full profile provider parameters in the provider configuration file.

The following table illustrates the Liberty profile attributes and the equivalent full profile parameters for the `oauthProvider` element.

*Table 133. Liberty `oauthProvider` element*

Liberty attribute name	Full profile equivalent parameter
<code>authorizationGrantLifetime</code>	<code>oauth20.max.authorization.grant.lifetime.seconds</code>
<code>authorizationCodeLifetime</code>	<code>oauth20.code.lifetime.seconds</code>

Table 133. Liberty oauthProvider element (continued)

Liberty attribute name	Full profile equivalent parameter
authorizationCodeLength	oauth20.code.length
accessTokenLifetime	oauth20.token.lifetime.seconds
accessTokenLength	oauth20.access.token.length
issueRefreshToken	oauth20.issue.refresh.token
refreshTokenLength	oauth20.refresh.token.length
mediatorClassname	oauth20.mediator.classnames
allowPublicClients	oauth20.allow.public.clients
grantType	oauth20.grant.types.allowed
authorizationFormTemplate	oauth20.authorization.form.template
authorizationErrorTemplate	oauth20.authorization.error.template
customLoginURL	oauth20.authorization.loginURL
autoAuthorizeParam	oauth20.autoauthorize.param
autoAuthorizeClient	oauth20.autoauthorize.clients
clientURISubstitutions	oauth20.client.uri.substitutions
filter	Filter
oauthOnly	oauthOnly
includeTokenInSubject	includeToken
characterEncoding	characterEncoding
clientTokenCacheSize	oauth20.token.userClientTokenLimit

The following table illustrates the Liberty attributes and the equivalent full profile parameters for the databaseStore element.

Table 134. Liberty databaseStore element

Liberty attribute name	Full profile equivalent parameter
cleanupExpiredTokenInterval	oauthjdbc.CleanupInterval

## Configuring automatic authorization: 8.5.5.0 Before you begin

Ensure that you enabled the OAuth 2.0 feature and configured an OAuth service provider by following Defining an OAuth service provider.

### About this task

You can authorize an OAuth client without the approval of the resource owner by enabling the automatic authorization feature of the WebSphere Application Server OAuth service provider.

### Procedure

To configure auto consent, use the autoAuthorizeParam attribute and the <autoAuthorizeClient> subelement of the <oauthProvider> element in the server.xml file:

```
<oauthProvider id="OAuthConfigSample" autoAuthorizeParam="autoauthz" ...>
  ...
  <autoAuthorizeClient>client01</autoAuthorizeClient>
  <autoAuthorizeClient>client02</autoAuthorizeClient>
</oauthProvider>
```

## Results

The `client01` and `client02` OAuth clients are configured for automatic authorization.

### OAuth endpoint URLs: **8.5.5.0**

After OAuth 2.0 is enabled, several endpoint URLs are configured on your WebSphere Application Server so that OAuth clients can communicate with the OAuth service provider before accessing OAuth protected resources.

The following endpoint URLs are configured for the OAuth service provider:

- Authorization endpoint URL

`https://host_name:port_number/oauth2/endpoint/provider_name/authorize`

where

- `host_name` is the host name of the OAuth service provider.
- `port_number` is the secure port number that is configured on the WebSphere Application Server.
- `provider_name` is the OAuth provider name.

- Token endpoint URL

`https://host_name:port_number/oauth2/endpoint/provider_name/token`

where

- `host_name` is the host name of the OAuth service provider.
- `port_number` is the secure port number that is configured on the WebSphere Application Server.
- `provider_name` is the OAuth provider name.

- Authorization endpoint URL of trust association interceptor (TAI) based user authentication

`https://host_name:port_number/oauth2/declaritiveEndpoint/provider_name/authorize`

where

- `host_name` is the host name of the OAuth service provider.
- `port_number` is the secure port number that is configured on the WebSphere Application Server.
- `provider_name` is the OAuth provider name.

By using this authorization endpoint, the applicable user authentication includes TAI.

### OAuth 2.0 service invocation

#### **8.5.5.0**

A registered OAuth client can invoke the WebSphere Application Server OAuth service authorization endpoint to request an access token. A registered OAuth client can also invoke the WebSphere Application Server OAuth service token endpoint to request an access token. The client then can use the access token to request protected web resources from WebSphere Application Server.

WebSphere Application Server OAuth 2.0 service supports the following flows.

#### Authorization code flow

Invoke authorization endpoint to request authorization code.

The OAuth client redirects the resource owner or user to the WebSphere Application Server OAuth 2.0 Authorization Service by adding its client id, client secret, state, redirect URI, and the optional scopes.

`https://host_name:port_number/oauth2/endpoint/provider_name/authorize`

or

`https://host_name:port_number/oauth2/declarativeEndpoint/provider_name/authorize`

Invoke OAuth token endpoint to request access token.

The OAuth client requests an access token from the WebSphere Application Server OAuth 2.0 token endpoint by adding `authorization_code` grant type, authorization code, `redirect_url`, and `client_id` as request parameters.

`https://host_name:port_number/oauth2/endpoint/provider_name/token`

The following example shows the constructions of the URIs when using authorization code, and the use of the access token to access web resources:

```
String charset = "UTF-8";
String param1 = "code";

if (isAuthorizationCode){
    String query = String.format("response_type=%s&
                                client_id=%s&
                                client_secret=%s&
                                state=%s&
                                redirect_uri=%s&
                                scope=%s",
                                URLEncoder.encode(param1, charset),
                                URLEncoder.encode(clientId, charset),
                                URLEncoder.encode(clientSecret, charset),
                                URLEncoder.encode(state, charset),
                                URLEncoder.encode(redirectURI, charset),
                                URLEncoder.encode(scope, charset));

    String s = authorizationEndPoint + "?" + query;
    System.out.println("Visit: " + s + "\nand grant permission");
    System.out.print("Now enter the OAuth code you have received in redirect uri :");
    BufferedReader br = new BufferedReader(new InputStreamReader(System.in));
    String code = br.readLine();
    param1 = "authorization_code";
    query = String.format("grant_type=%s&
                            code=%s&
                            client_id=%s&
                            client_secret=%s&
                            state=%s&
                            redirect_uri=%s&
                            scope=%s",
                            URLEncoder.encode(param1, charset),
                            URLEncoder.encode(code, charset),
                            URLEncoder.encode(clientId, charset),
                            URLEncoder.encode(clientSecret, charset),
                            URLEncoder.encode(state, charset),
                            URLEncoder.encode(redirectURI, charset),
                            URLEncoder.encode(scope, charset));

    URL url = new URL(tokenEndPoint);
    HttpURLConnection con = (HttpURLConnection)url.openConnection();
    con.setRequestProperty("Content-Type", "application/x-www-form-urlencoded;charset=" + charset);
    con.setDoOutput(true);
    con.setRequestMethod("POST");
    OutputStream output = null;
    try {
        output = con.getOutputStream();
        output.write(query.getBytes(charset));
        output.flush();
    } finally {
        if (output != null) try {
            output.close();
        } catch (IOException logOrIgnore) {}
    }
    con.connect();
    System.out.println("response message is = " + con.getResponseMessage());
    // read the output from the server
    BufferedReader reader = null;
    StringBuilder stringBuilder;
    reader = new BufferedReader(new InputStreamReader(con.getInputStream()));
    stringBuilder = new StringBuilder();
    String line = null;
    try {
        while ((line = reader.readLine()) != null) {
```

```

        stringBuilder.append(line + "\n");
    }
} finally {
    if (reader != null) try {
        reader.close();
    } catch (IOException logOrIgnore) {}
}
String tokenResponse = stringBuilder.toString();
System.out.println ("response is = " + tokenResponse);
JSONObject json = JSONObject.parse(tokenResponse);
if (json.containsKey("access_token")) {
    accessToken = (String)json.get("access_token");
    this.accessToken = accessToken;
}
if (json.containsKey("refresh_token")) {
    refreshToken = (String)json.get("refresh_token");
}
//sendRequestForAccessToken(query);
if (accessToken != null) {
    String query = String.format("access_token=%s",
        URLEncoder.encode(accessToken, charset));
    URL urlResource = new URL(resourceEndPoint);
    HttpURLConnection conn = (HttpURLConnection) urlResource.openConnection();
    conn.setRequestMethod("POST");
    conn.setRequestProperty("Content-type", "application/x-www-form-urlencoded");
    conn.setDoOutput(true);
    output = null;
    try {
        output = conn.getOutputStream();
        output.write(query.getBytes(charset));
        output.flush();
    } finally {
        if (output != null) try {
            output.close();
        } catch (IOException logOrIgnore) {}
    }
    conn.connect();
    System.out.println("response to the resource request is = " + conn.getResponseMessage ());
    reader = null;
    if(conn.getResponseCode()>=200 && conn.getResponseCode() < 400) {
        reader = new BufferedReader(new InputStreamReader(conn.getInputStream()));
        stringBuilder = new StringBuilder();
        String line = null;
        try {
            while ((line = reader.readLine()) != null) {
                stringBuilder.append(line + "\n");
            }
        } finally {
            if (reader != null) try {
                reader.close();
            } catch (IOException logOrIgnore) {}
        }
        System.out.println ("response message to the request resource is = " + stringBuilder.toString());
    } else {
        isValidResponse = false;
    }
}
}
}

```

## Implicit grant flow

The OAuth client requests an access token from the WebSphere Application Server OAuth 2.0 authorization endpoint by adding token response\_type, redirect\_url, client\_id, scope, and state as request parameters.

`https://host_name:port_number/oauth2/endpoint/provider_name/authorize`

or

`https://host_name:port_number/oauth2/declarativeEndpoint/provider_name/authorize`

The following example shows the construction of the URI when using implicit grant:

```

if (isImplicit) {
    param1 = "token";
    String query = String.format("response_type=%s&
                                client_id=%s&
                                state=%s&
                                redirect_uri=%s&
                                scope=%s",
                                URLEncoder.encode(param1, charset),
                                URLEncoder.encode(clientId, charset),
                                URLEncoder.encode(state, charset),
                                URLEncoder.encode(redirectURI, charset),
                                URLEncoder.encode(scope, charset));

    String s = authorizationEndPoint + "?" + query;
    System.out.println("Visit: " + s + "\nand grant permission");
    System.out.print("Now enter the access token you have received in redirect uri :");
    BufferedReader br = new BufferedReader(new InputStreamReader(System.in));
    accessToken = br.readLine();
    if (accessToken != null) {
        // send Resource Request using the access token
    }
}
}

```

## Client credential flow

The OAuth client accesses the token endpoint by using the client ID and client secret, and exchanges for an access token for future resource requests. In this flow, the client accesses the token endpoint by adding `client_credentials` grant type, `client_id`, and `client_secret` as request parameters.

[https://host\\_name:port\\_number/oauth2/endpoint/provider\\_name/token](https://host_name:port_number/oauth2/endpoint/provider_name/token)

The following example shows the construction of the URI when using client credential:

```

if (isClientCredentials){
    param1 = "client_credentials";
    String query = String.format("grant_type=%s&
                                scope=%s&
                                client_id=%s&
                                client_secret=%s",
                                URLEncoder.encode(param1, charset),
                                URLEncoder.encode(scope, charset),
                                URLEncoder.encode(clientId, charset),
                                URLEncoder.encode(clientSecret, charset));

    accessToken = sendRequestForAccessToken(query);
    if (accessToken != null) {
        //send Resource Request using (accessToken);
    }
}
}

```

## Resource owner password credentials flow

The Resource Owner Password Credentials flow passes the user ID and password of the resource owner to the token endpoint directly. In this flow, The OAuth client accesses the token endpoint by adding `password` grant type, `client_id`, `client_secret`, `username`, `password`, `scope`, and `state` as request parameters.

[https://host\\_name:port\\_number/oauth2/endpoint/provider\\_name/token](https://host_name:port_number/oauth2/endpoint/provider_name/token)

The following example shows the construction of the URI when using resource owner password:

```

if (isResourceOwnerCredentials) {
    param1 = "password";
    String query = String.format("grant_type=%s&
                                username=%s&

```

```

        password=%s&
        scope=%s&
        client_id=%s&
        client_secret=%s",
        URLEncoder.encode(param1, charset),
        URLEncoder.encode(resOwnerName, charset),
        URLEncoder.encode(resOwnerPassword, charset),
        URLEncoder.encode(scope, charset),
        URLEncoder.encode(clientId, charset),
        URLEncoder.encode(clientSecret, charset));
    accessToken = sendRequestForAccessToken(query);
    if (accessToken != null) {
        //send Resource Request using (accessToken);
    }
}

```

If the access token is expired, then the refresh token can be sent to get a valid access token. The following example shows how to send a refresh token:

```

if(isAccessToken) {
    if (this.accessToken != null) {
        if (!sendResourceRequest(this.accessToken)) {
            // resource request failed...
            //get refresh token
            param1 = "refresh_token";
            String query = String.format("grant_type=%s&
                client_id=%s&
                client_secret=%s&
                refresh_token=%s&
                scope=%s",
                URLEncoder.encode(param1, charset),
                URLEncoder.encode(clientId, charset),
                URLEncoder.encode(clientSecret, charset),
                URLEncoder.encode(this.refreshToken, charset),
                URLEncoder.encode(scope, charset));

            accessToken = sendRequestForAccessToken(query);
            if (accessToken != null) {
                sendResourceRequest(accessToken);
            }
        }
    }
}
}

```

## Customizing an OAuth provider

**8.5.5.0**

The WebSphere Application Server OAuth service provider has plug-in points for customization. You can replace the default form login page for user authentication, or develop your own user consent form to collect client authorization data. WebSphere Application Server OAuth providers also allow customized post processing for major events in OAuth token issuing by using mediators.

### Custom mediator: **8.5.5.0**

An OAuth 2.0 mediator is used as a callback during the OAuth 2.0 message processing to perform customized post processing.

## Write an OAuth 2.0 mediator

To write a mediator, you must implement the interface named `com.ibm.oauth.core.api.oauth20.mediator.OAuth20Mediator`. You can implement one or more of the following methods to perform custom post processing.

```
void init(OAuthComponentConfiguration config)
```

This method is called by a factory when an instance of this object is created.

```
void mediateAuthorize(AttributeList attributeList)
```

This method is called by the core component after basic message validation and processing to allow any post custom processing by the component consumer in the `processAuthorization` method.

```
void mediateAuthorizeException(AttributeList attributeList, OAuthException exception)
```

This method is called by the core component when the protocol exception happens to allow any post custom processing by the component consumer in the `processAuthorization` method.

```
void mediateResource(AttributeList attributeList)
```

This method is called by the core component after basic message validation and processing to allow any post custom processing by the component consumer in the `processResourceRequest` method.

```
void mediateResourceException(AttributeList attributeList, OAuthException exception)
```

This method is called by the core component when protocol exception happens to allow any post custom processing by the component consumer in the `processResourceRequest` method.

```
void mediateToken(AttributeList attributeList)
```

This method is called by the core component after basic message validation and processing to allow any post custom processing by the component consumer in the `processTokenRequest` method.

```
void mediateTokenException(AttributeList attributeList, OAuthException exception)
```

This method is called by the core component when protocol exception happens to allow any post custom processing by the component consumer in the `processTokenRequest` method.

## Enable OAuth 2.0 mediator for an OAuth provider

To add a customized mediator to a specific OAuth 2.0 service provider, update the provider definition in the `server.xml` file. Add the `mediatorClassname` attribute of the `oauthProvider` element and specify the class name for the mediator. You can also specify multiple class names for mediators by using the `mediatorClassname` subelement of the `oauthProvider` element. If multiple mediators are specified, those mediators are started in the order they are specified. You must also define a `library` element that contains the mediator class and refer to the library with the `libraryRef` attribute.

The following example shows a sample custom mediator entry in the provider definition in the `server.xml` file:

```
<oauthProvider id="OAuthConfigSample" libraryRef="myLib"
  mediatorClassname="com.ibm.ws.security.oauth20.mediator.ResourceOwnerValidationMediator" ...>
  ...
</oauthProvider>

<library id="myLib">
  <fileset dir="C:\mydir" includes="myLib.jar" />
</library>
```

The following code sample implements the credential validation by using the WebSphere Application Server user registry in the resource owner password credentials flow.

```

package com.ibm.ws.security.oauth20.mediator;

import com.ibm.oauth.core.api.attributes.AttributeList;
import com.ibm.oauth.core.api.config.OAuthComponentConfiguration;
import com.ibm.oauth.core.api.error.OAuthException;
import com.ibm.oauth.core.api.error.oauth20.OAuth20MediatorException;
import com.ibm.oauth.core.api.oauth20.mediator.OAuth20Mediator;
import com.ibm.oauth.core.internal.oauth20.OAuth20Constants;
import com.ibm.websphere.security.CustomRegistryException;
import com.ibm.websphere.security.PasswordCheckFailedException;
import com.ibm.websphere.security.UserRegistry;

import java.rmi.RemoteException;
import java.util.logging.Level;
import java.util.logging.Logger;

import javax.naming.InitialContext;
import javax.naming.NamingException;

public class ResourceOwnerValidationMediator implements OAuth20Mediator {
    private static final String CLASS = ResourceOwnerValidationMediator.class.getName();
    private static final Logger LOG = Logger.getLogger(CLASS);
    private UserRegistry reg = null;

    public void init(OAuthComponentConfiguration config) {
        try {
            InitialContext ctx = new InitialContext();
            reg = (UserRegistry) ctx.lookup("UserRegistry");
        } catch (NamingException ne) {
            LOG.log(Level.SEVERE, "Cannot lookup UserRegistry", ne);
        }
    }

    public void mediateAuthorize(AttributeList attributeList)
        throws OAuth20MediatorException {
        // nothing to do here
    }

    public void mediateAuthorizeException(AttributeList attributeList,
        OAuthException exception)
        throws OAuth20MediatorException {
        // nothing to do here
    }

    public void mediateResource(AttributeList attributeList)
        throws OAuth20MediatorException {
        // nothing to do here
    }

    public void mediateResourceException(AttributeList attributeList,
        OAuthException exception)
        throws OAuth20MediatorException {
        // nothing to do here
    }

    public void mediateToken(AttributeList attributeList)
        throws OAuth20MediatorException {
        final String methodName = "mediateToken";
        LOG.entering(CLASS, methodName, attributeList);
        if("password".equals(attributeList.getAttributeValueByName("grant_type"))) {
            String username = attributeList.getAttributeValueByName("username");
            String password = attributeList.getAttributeValueByName("password");
            try {

```

```

        reg.checkPassword(username, password);
    } catch (PasswordCheckFailedException e) {
        throw new OAuth20MediatorException("User doesn't exist or the
   password doesn't match.", e);
    } catch (CustomRegistryException e) {
        throw new OAuth20MediatorException("Cannot validate resource owner.", e);
    } catch (RemoteException e) {
        throw new OAuth20MediatorException("Cannot validate resource owner.", e);
    }
}
LOG.exiting(CLASS, methodName);
}

public void mediateTokenException(AttributeList attributeList,
                                 OAuthException exception)
    throws OAuth20MediatorException {
    final String methodName = "mediateTokenException";
    LOG.entering(CLASS, methodName, new Object[] {attributeList, exception});
    if("password".equals(attributeList.getAttributeValueByName("grant_type"))) {
        // clear sensitive data
        attributeList.setAttribute("access_token",
                                   OAuth20Constants.ATTRTYPE_RESPONSE_ATTRIBUTE,
                                   new String[0]);
        attributeList.setAttribute("refresh_token",
                                   OAuth20Constants.ATTRTYPE_RESPONSE_ATTRIBUTE,
                                   new String[0]);
    }
    LOG.exiting(CLASS, methodName);
}
}
}

```

### Custom consent form template: **8.5.5.0**

The OAuth authorization server provides a template to acquire user consent information about which OAuth clients are authorized to access the protected resource in given scopes. The authorization request from the OAuth client includes a list of requested scopes from the template.

WebSphere Application Server allows the consent form template to be either a static HTML page or a dynamic web page. In both cases, the template must be provided as an unprotected web resource. The form retriever in WebSphere Application Server integration does not perform any authentication when accessing this template URL.

The WebSphere Application Server OAuth provider includes a sample consent form template, and allows customization by using `oauthFormData` variable.

To customize the consent form, you must edit the `oauthFormData` variable by using JavaScript. The following variables are included in the form data:

- `authorizationUrl` - the authorization URL where the form is being submitted
- `clientDisplayName` - the display name of the client
- `nonce` - random generated number to prevent cross-site request forgery (CSRF)
- `client_id` - see the OAuth 2.0 specification
- `response_type` - see the OAuth 2.0 specification
- `redirect_uri` - see the OAuth 2.0 specification
- `state` - see the OAuth 2.0 specification
- `scope` - see the OAuth 2.0 specification

The developer of a form template must include the content of the `oauthFormData` variable, by using JavaScript. The developer must interpret the scope value to be a meaningful value to a user. When a user authorizes the request, the developer can call the `submitForm(oauthFormData)` method to perform the authorization. The `submitForm` method is provided by default. However, if developers are familiar with OAuth 2.0 protocol, they can implement their own function to submit the OAuth authorization request.



8.5.5.4

A `cancel(oauthFormData)` method is provided by default and can be used to allow a user to cancel the authorization request.



8.5.5.4

The consent form can also be modified to allow the user's consent selection to be cached. This means that if the same OpenID Connect client makes a new authorization request with the same approved scopes or reduced scopes, the user is not be prompted with the consent form. Instead, the previously allowed scopes are considered authorized and passed to the protected resource accordingly.



8.5.5.4

If client registration is in `localStorage` mode, the user's consent selection is cached in the browser session. The approved scopes remain cached for the given user until the session is closed or until a set amount of time (specified in the server configuration) has elapsed.



8.5.5.4

If client registration is in `databaseStore` mode, the user's consent selection can be persistent in a database table, `OAuthDBSchema.OAUTH20CONSENTCACHE`. The scopes remain cached for the given user until a set amount of time (specified in the server configuration) has elapsed. The OpenID Connect provider tries to create the consent cache table automatically, but it is suggested that the user explicitly create the consent table when configuring a database for an OAuth2.0 provider and OpenID Connect provider, see [Persistent OAuth service configuration](#) for further details.



8.5.5.4

To use this functionality, the developer of a form template must include a `prompt` value within the `oauthFormData` JavaScript object. In order to cache the user's affirmative response and prevent the consent form from being displayed again in the same session, the `prompt` value is set to the string `none`. To allow the user to submit an affirmative response without caching the approval, the `prompt` value is set to the string `consent`.

You can use a dynamic page that returns globalized content according to the `Accept-Language` header in the request. When retrieving the template, the `Accept-Language` header is forwarded, and the template developer must decide which content to return regarding the preferred language.

**Note:** The `clientDisplayName` variable is not escaped in HTML. The template developer must sanitize the value, as the value is input by a user during client registration.

To use a custom consent form template page for a specific OAuth 2.0 service provider, you must update the service provider definition in the `server.xml` file. In the provider configuration, you must use the `authorizationFormTemplate` attribute of the `oauthProvider` element and add the template URL as the value. The following example shows a sample template entry in the provider configuration:

```
<oauthProvider id="OAuthConfigSample"
  authorizationFormTemplate="https://acme.com:9043/oath20/template.html
  ...>
```

The following example illustrates a sample consent form:

```
<oauthProvider id="OAuthConfigSample"
  authorizationLoginURL="https://acme.com:9043/oath20/login.jsp"
  ...>
```

```
function escapeHTML(str) {
  var ele = document.createElement("div");
  ele.innerText = ele.textContent = str;
  return ele.innerHTML;
```

```

}
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>OAuth authorization form</title>
<script language="javascript">
function init() {
  var scope = oauthFormData.scope;
  var scopeEle = document.getElementById("oauth_scope");
  var ul = document.createElement("ul");
  if(scope) {
    for(var i=0; i< scope.length; i++) {
      var n = document.createElement("li");
      n.innerHTML = scope[i];
      ul.appendChild(n);
    }
  }
  scopeEle.appendChild(ul);
  // set client name
  var clientEle = document.getElementById("client_name");
  clientEle.innerHTML = escapeHTML(oauthFormData.clientDisplayName);
}

function escapeHTML(str) {
  var ele = document.createElement("div");
  ele.innerText = ele.textContent = str;
  return ele.innerHTML;
}
</script>
</head>
<body onload="init()">
  <div>Do you want to allow client <span id=client_name style="font-weight:bold">xxxxxxx</span> to access your data?</div>
  <div id="oauth_scope">
  </div>
  <div>
    <form action="javascript:submitForm(oauthFormData);">
      <input type="submit" value="Allow, remember my decision" onclick="javascript:oauthFormData.prompt = 'none';"/>
      <input type="submit" value="Allow once" onclick="javascript:oauthFormData.prompt = 'consent';"/>
      <input type="button" value="Cancel" onclick="javascript:cancel(oauthFormData);"/>
    </form>
  </div>
</body>
</html>

```

## Custom user login form: **8.5.5.0**

The WebSphere Application Server OAuth service provider includes a form login page for a user to submit a user name and password.

You can customize your own form login page, but it must be implemented as required in the form-based authentication in the servlet specification. In this form, the action must be `j_security_check`, and use the `j_username` input field to get the user name. The action must also use the `j_password` input field to get the user password. The custom form login page must be provided as an unprotected web resource.

To use the custom form login page for a specific OAuth20 service provider, you must update the service provider definition in the `server.xml` file. In the provider configuration, you must add the `customLoginURL` attribute and specify the login page URL as the value.

The following is an example custom login page entry in the provider definition:

```

<oauthProvider id="OAuthConfigSample"
  customLoginURL="https://acme.com:9043/oauth20/login.jsp"
  ...>

```

**Note:** Make sure that any files included in your form-login page (such as external style sheets, or images) are unprotected.

## Persistent OAuth service configuration

8.5.5.0

WebSphere Application Server supports a persistent OAuth 2.0 service by persisting OAuth tokens and clients in a database. With persistent OAuth 2.0 services, an authorized client can access OAuth 2.0 service after OAuth services are restarted.

To configure persistent OAuth 2.0 services, complete the following steps:

### 1. Configure the OAuth 2.0 service provider.

To use a database store, you must specify the `<databaseStore>` subelement of the `<oauthProvider>` element. The only required attribute on the `<databaseStore>` element is `<dataSourceRef>`, whose value must be the id of the `<dataSource>` element.

The following example is a sample `server.xml` file for an OAuth provider that uses a Derby database store:

```
<server>

  <featureManager>
    <feature>oauth-2.0</feature>
    <feature>ssl-1.0</feature>
    <feature>jdbc-4.0</feature>
    <feature>jndi-1.0</feature>
  </featureManager>

  <keyStore password="keyspass" />

  <oauth-roles>
    <authenticated>
      <user>testuser</user>
    </authenticated>
  </oauth-roles>

  <oauthProvider id="OAuthConfigDerby" filter="request-uri%ssodemo"
    oauthOnly="false">
    <databaseStore dataSourceRef="OAuthFvtDataSource" />
  </oauthProvider>

  <jdbcDriver id="DerbyEmbedded" libraryRef="DerbyLib" />

  <library id="DerbyLib" fileSetRef="DerbyFileset" />

  <fileset id="DerbyFileset" dir="{DERBY_JDBC_DRIVER_PATH}"
    includes="derby.jar" />

  <dataSource id="OAuthFvtDataSource" jndiName="jdbc/OAuth2DB"
    jdbcDriverRef="DerbyEmbedded">
    <properties.derby.embedded databaseName="D:\oauth2db"
      createDatabase="create" />
  </dataSource>

  <webAppSecurity allowFailOverToBasicAuth="true" />

  <basicRegistry id="basic" realm="BasicRealm">
    <user name="testuser" password="testuserpwd" />
  </basicRegistry>

</server>
```

### 2. Set up a database and table to store the OAuth token and client.

- a. Create a database for persistent OAuth service. See the vendor documentation for database creation. In this example, the database name is `D:\oauth2db`.

b. Create 3 OAuth tables as defined by the following SQL statements:

```
----- CREATE TABLES -----
CREATE TABLE OAuthDBSchema.OAUTH2OCACHE
(
  LOOKUPKEY VARCHAR(256) NOT NULL,
  UNIQUEID VARCHAR(128) NOT NULL,
  COMPONENTID VARCHAR(256) NOT NULL,
  TYPE VARCHAR(64) NOT NULL,
  SUBTYPE VARCHAR(64),
  CREATEDAT BIGINT,
  LIFETIME INT,
  EXPIRES BIGINT,
  TOKENSTRING VARCHAR(2048) NOT NULL,
  CLIENTID VARCHAR(64) NOT NULL,
  USERNAME VARCHAR(64) NOT NULL,
  SCOPE VARCHAR(512) NOT NULL,
  REDIRECTURI VARCHAR(2048),
  STATEID VARCHAR(64) NOT NULL,
  EXTENDEDFIELDS CLOB NOT NULL DEFAULT '{}')
);

CREATE TABLE OAuthDBSchema.OAUTH2OCLIENTCONFIG
(
  COMPONENTID VARCHAR(256) NOT NULL,
  CLIENTID VARCHAR(256) NOT NULL,
  CLIENTSECRET VARCHAR(256),
  DISPLAYNAME VARCHAR(256) NOT NULL,
  REDIRECTURI VARCHAR(2048),
  ENABLED INT,
  CLIENTMETADATA CLOB NOT NULL DEFAULT '{}')
);

CREATE TABLE OAuthDBSchema.OAUTH2OCONSENTCACHE
(
  CLIENTID VARCHAR(256) NOT NULL,
  USERID VARCHAR(256),
  PROVIDERID VARCHAR(256) NOT NULL,
  SCOPE VARCHAR(1024) NOT NULL,
  EXPIRES BIGINT,
  EXTENDEDFIELDS CLOB NOT NULL DEFAULT '{}')
);

----- ADD CONSTRAINTS -----
ALTER TABLE OAuthDBSchema.OAUTH2OCACHE
  ADD CONSTRAINT PK_LOOKUPKEY PRIMARY KEY (LOOKUPKEY);

ALTER TABLE OAuthDBSchema.OAUTH2OCLIENTCONFIG
  ADD CONSTRAINT PK_COMPIDCLIENTID PRIMARY KEY (COMPONENTID,CLIENTID);

----- CREATE INDEXES -----
CREATE INDEX OAUTH2OCACHE_EXPIRES ON OAUTHDBSCHEMA.OAUTH2OCACHE (EXPIRES ASC);
```

3. Configure WebSphere Application Server.

Configure the WebSphere Application Server data source. You must set the data source Java Naming and Directory Interface (JNDI) name to be jdbc/OAuth2DB. The JNDI name must match the jndiName attribute of the <dataSource> element in the server.xml file. Enter the database name, for example, D:\oauth2db.

For more information about the configuration of DB2 and Derby for OAuth persistent services, see IBM DB2 for persistent OAuth services and Derby database for persistent OAuth services. You can use them as a sample template to configure other databases.

4. Add the registered OAuth clients to the database.

To persist a client in a database, you must save the client to the database. The following SQL statements add the dbclient01 and dbclient02 OAuth clients to a Derby database:

```

CONNECT 'jdbc:derby:D:\oauth2db';
INSERT INTO OAuthDBSchema.OAUTH2CLIENTCONFIG VALUES
(
  'OAuthConfigDerby',
  'dbclient01',
  'secret',
  'dbclient01',
  'http://localhost:9080/oauthclient/redirect.jsp',
  1
),
(
  'OAuthConfigDerby',
  'dbclient02',
  'secret',
  'dbclient02',
  'http://localhost:9080/oauthclient/redirect.jsp',
  1
);
DISCONNECT CURRENT;

```

**Note:** **8.5.5.2** The Componentid must be the same as the id of the oauthProvider element in the server.xml file.

### Derby database for persistent OAuth services: **8.5.5.0**

Derby database can be used for persistent OAuth services. For convenience and reference purposes, this topic documents the steps you need to configure Derby database, either remote or local to the OAuth service, for OAuth persistent service.

To configure Derby database for persistent OAuth services, complete the following steps:

1. Create a database and tables.

Edit and run the following SQL statement to create an OAuth database and table:

```

--- Change oauth2db to the name you want for the database
--- Connect to Derby, choose one connection option to uncomment
--- if connecting to Derby as network server
--- CONNECT 'jdbc:derby://localhost:1527/oauth2db;create=true';

--- if connecting to embedded derby, you can change D:\oauth2db to location of database
--- CONNECT 'jdbc:derby:D:\oauth2db;create=true';

--- if creating tables in existing Derby database, remove the create=true parameter.

----- CREATE TABLES -----
CREATE TABLE OAuthDBSchema.OAUTH2OCACHE (
  LOOKUPKEY VARCHAR(256) NOT NULL,
  UNIQUEID VARCHAR(128) NOT NULL,
  COMPONENTID VARCHAR(256) NOT NULL,
  TYPE VARCHAR(64) NOT NULL,
  SUBTYPE VARCHAR(64),
  CREATEDAT BIGINT,
  LIFETIME INT,
  EXPIRES BIGINT,
  TOKENSTRING VARCHAR(2048) NOT NULL,
  CLIENTID VARCHAR(64) NOT NULL,
  USERNAME VARCHAR(64) NOT NULL,
  SCOPE VARCHAR(512) NOT NULL,
  REDIRECTURI VARCHAR(2048),
  STATEID VARCHAR(64) NOT NULL,
  EXTENDEDFIELDS CLOB NOT NULL DEFAULT '{}')
);

```

```

CREATE TABLE OAuthDBSchema.OAUTH2CLIENTCONFIG (
  COMPONENTID VARCHAR(256) NOT NULL,
  CLIENTID VARCHAR(256) NOT NULL,
  CLIENTSECRET VARCHAR(256),
  DISPLAYNAME VARCHAR(256) NOT NULL,
  REDIRECTURI VARCHAR(2048),
  ENABLED INT,
  CLIENTMETADATA CLOB NOT NULL DEFAULT '{}')
);

CREATE TABLE OAuthDBSchema.OAUTH2CONSENTCACHE (
  CLIENTID VARCHAR(256) NOT NULL,
  USERID VARCHAR(256),
  PROVIDERID VARCHAR(256) NOT NULL,
  SCOPE VARCHAR(1024) NOT NULL,
  EXPIRES BIGINT,
  EXTENDEDFIELDS CLOB NOT NULL DEFAULT '{}')
);

----- ADD CONSTRAINTS -----
ALTER TABLE OAuthDBSchema.OAUTH2CACHE
  ADD CONSTRAINT PK_LOOKUPKEY PRIMARY KEY (LOOKUPKEY);

ALTER TABLE OAuthDBSchema.OAUTH2CLIENTCONFIG
  ADD CONSTRAINT PK_COMPIDCLIENTID PRIMARY KEY (COMPONENTID,CLIENTID);

----- CREATE INDEXES -----
CREATE INDEX OAUTH2CACHE_EXPIRES ON OAUTHDBSCHEMA.OAUTH2CACHE (EXPIRES ASC);

DISCONNECT CURRENT;

```

Run the createTables.sql file by starting **ij** with the following command:

```
ij createTables.sql
```

## 2. Configure the WebSphere Application Server Liberty server.

The following example is a sample server.xml file for an OAuth provider that uses a Derby database store:

```

<server>

  <featureManager>
    <feature>oauth-2.0</feature>
    <feature>ssl-1.0</feature>
    <feature>jdbc-4.0</feature>
    <feature>jndi-1.0</feature>
  </featureManager>

  <keyStore password="keyspass" />

  <oauth-roles>
    <authenticated>
      <user>testuser</user>
    </authenticated>
  </oauth-roles>

  <oauthProvider id="OAuthConfigDerby" filter="request-url%ssodemo"
    oauthOnly="false">
    <databaseStore dataSourceRef="OAuthDerbyDataSource" />
  </oauthProvider>

  <jdbcDriver id="DerbyEmbedded" libraryRef="DerbyLib" />

  <library id="DerbyLib" filesetRef="DerbyFileset" />

  <fileset id="DerbyFileset" dir="${DERBY_JDBC_DRIVER_PATH}"

```

```

        includes="derby.jar" />

<dataSource id="OAuthDerbyDataSource" jndiName="jdbc/OAuth2DB"
            jdbcDriverRef="DerbyEmbedded">
    <properties.derby.embedded databaseName="D:\oauth2db"
                            createDatabase="create" />
</dataSource>

<webAppSecurity allowFailOverToBasicAuth="true" />

<basicRegistry id="basic" realm="BasicRealm">
    <user name="testuser" password="testuserpwd" />
</basicRegistry>
</server>

```

**Note:** **8.5.5.2** The Componentid must be the same as the id of the oauthProvider element in the server.xml file.

### IBM DB2 for persistent OAuth services: **8.5.5.0**

IBM DB2 can be used for persistent OAuth services. For convenience and reference purposes, this topic documents the steps you need to configure DB2 for OAuth persistent service.

To configure DB2 for persistent OAuth services, complete the following steps:

1. Create a database and tables.

Edit and run the following SQL statement to create an OAuth database and table:

```

-- Change oauth2db to the name you want for the database

CREATE DATABASE oauth2db USING CODESET UTF8 TERRITORY US;
CONNECT TO oauth2db;

---- CREATE TABLES ----
CREATE TABLE OAuthDBSchema.OAUTH20CACHE
(
    LOOKUPKEY VARCHAR(256) NOT NULL,
    UNIQUEID VARCHAR(128) NOT NULL,
    COMPONENTID VARCHAR(256) NOT NULL,
    TYPE VARCHAR(64) NOT NULL,
    SUBTYPE VARCHAR(64),
    CREATEDAT BIGINT,
    LIFETIME INT,
    EXPIRES BIGINT,
    TOKENSTRING VARCHAR(2048) NOT NULL,
    CLIENTID VARCHAR(64) NOT NULL,
    USERNAME VARCHAR(64) NOT NULL,
    SCOPE VARCHAR(512) NOT NULL,
    REDIRECTURI VARCHAR(2048),
    STATEID VARCHAR(64) NOT NULL
    EXTENDEDFIELDS CLOB NOT NULL DEFAULT '{}';
);

CREATE TABLE OAuthDBSchema.OAUTH20CLIENTCONFIG
(
    COMPONENTID VARCHAR(256) NOT NULL,
    CLIENTID VARCHAR(256) NOT NULL,
    CLIENTSECRET VARCHAR(256),
    DISPLAYNAME VARCHAR(256) NOT NULL,
    REDIRECTURI VARCHAR(2048),
    ENABLED INT
    CLIENTMETADATA CLOB NOT NULL DEFAULT '{}';
);

```

```

CREATE TABLE OAuthDBSchema.OAUTH20CONSENTCACHE (
  CLIENTID VARCHAR(256) NOT NULL,
  USERID VARCHAR(256),
  PROVIDERID VARCHAR(256) NOT NULL,
  SCOPE VARCHAR(1024) NOT NULL,
  EXPIRES BIGINT,
  EXTENDEDFIELDS CLOB NOT NULL DEFAULT '{}')
);

---- ADD CONSTRAINTS ----
ALTER TABLE OAuthDBSchema.OAUTH20CACHE
  ADD CONSTRAINT PK_LOOKUPKEY PRIMARY KEY (LOOKUPKEY);

ALTER TABLE OAuthDBSchema.OAUTH20CLIENTCONFIG
  ADD CONSTRAINT PK_COMPIDCLIENTID PRIMARY KEY (COMPONENTID,CLIENTID);

---- CREATE INDEXES ----
CREATE INDEX OAUTH20CACHE_EXPIRES ON OAUTHDBSCHEMA.OAUTH20CACHE (EXPIRES ASC);

---- GRANT PRIVILEGES ----
---- UNCOMMENT THE FOLLOWING IF YOU USE AN ACCOUNT OTHER THAN ADMINISTRATOR FOR DB ACCESS ----

-- Change dbuser to the account you want to use to access your database
-- GRANT ALL ON OAuthDBSchema.OAUTH20CACHE TO USER dbuser;
-- GRANT ALL ON OAuthDBSchema.OAUTH20CLIENTCONFIG TO USER dbuser;

---- END OF GRANT PRIVILIGES ----

DISCONNECT CURRENT;

```

The default DB2 listening port is 50000. If you want to find it, run the following command and find the value of the SVCENAME parameter. If it is a number, then it is the port number. If it is a name, look for the name in the /etc/services file or the Windows equivalent if you are using Windows.

```

Linux/Unix: db2 get dbm cfg | grep SVCENAME
Windows:   db2 get dbm cfg | findstr SVCENAME

```

You can create a database and tables in DB2 by running the following statement:

```
db2 -tvf createTables.sql
```

## 2. Configure the WebSphere Application Server Liberty server.

The following example is a sample server.xml file for an OAuth provider that uses a DB2 store:

```

<server>
  <featureManager>
    <feature>oauth-2.0</feature>
    <feature>ssl-1.0</feature>
    <feature>jdbc-4.0</feature>
    <feature>jndi-1.0</feature>
  </featureManager>

  <keyStore password="keyspass" />

  <oauth-roles>
    <authenticated>
      <user>testuser</user>
    </authenticated>
  </oauth-roles>

  <oauthProvider id="DBOAuth20Provider" oauthOnly="true"
    filter="request-url%=AnnuityOAuthWeb/index.jsp">
    <databaseStore dataSourceRef="OAUTH2DBDS" />
  </oauthProvider>

```

```

<jdbcDriver id="db2Universal" libraryRef="DB2JCC4LIB" />
<library apiTypeVisibility="spec,ibm-api,third-party" filesetRef="db2jcc4"
  id="DB2JCC4LIB" />
<fileset dir="${shared.resource.dir}/db2" id="db2jcc4"
  includes="db2jcc4.jar db2jcc_license_cu.jar" />
<dataStore id="OAUTH2DBDS" jdbcDriverRef="db2Universal"
  jndiName="jdbc/oauthProvider">
  <properties.db2.jcc databaseName="OAUTH2DB" driverType="4"
    user="bob" password="abcdefg"
    portNumber="50000"
    serverName="db2.server.mycompany.com" />
</dataStore>
<webAppSecurity allowFailOverToBasicAuth="true" />
<basicRegistry id="basic" realm="BasicRealm">
  <user name="testuser" password="testuserpwd" />
</basicRegistry>
</server

```

The following example adds a client to DB2:

```

INSERT INTO OAuthDBSchema.OAUTH2CLIENTCONFIG
(
  COMPONENTID,
  CLIENTID,
  CLIENTSECRET,
  DISPLAYNAME,
  REDIRECTURI,
  ENABLED
)
VALUES
(
  'DBOAuth20Provider',
  'key',
  'secret',
  'My Client',
  'https://localhost:9443/oauth/redirect.jsp',
  1
)

```

**Note:** **8.5.5.2** The Componentid must be the same as the id of the oauthProvider element in the server.xml file.

---

## Configuring Common Secure Interoperability version 2 (CSIv2) in Liberty



**8.5.5.6**

Liberty supports CSIv2 security at various levels such as the message authentication (authentication layer), identity assertion (attribute layer), and client certificate authentication (transport layer). Using the CSIv2 feature, you can specify the type of authentication for both inbound and outbound requests to downstream servers. CSIv2 features are enabled automatically when the appSecurity-2.0 and ejbRemote-3.2 features are configured in the server.xml file. You can configure CSIv2 in Liberty to enable interoperability between Java Platform, Enterprise Edition vendors.

## Procedure

The following is the default configuration that is used without having to specify it in the `server.xml` file when the `appSecurity-2.0` and `ejbRemote-3.2` features are configured.

```
<orb id="defaultOrb">
  <serverPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Required"/>
      <transportLayer/>
    </layers>
  </serverPolicy.csiv2>
  <clientPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Supported"/>
      <transportLayer/>
    </layers>
  </clientPolicy.csiv2>
</orb>
```

You can change each of the layers in `serverPolicy.csiv2` and in `clientPolicy.csiv2` for customizing the inbound and outbound CSIV2 settings.

## Configuring inbound CSIV2 in Liberty



8.5.5.6

Common Secure Interoperability, version 2 (CSIV2) feature inbound configuration determines the type of accepted authentication for inbound requests. The CSIV2 feature is enabled automatically when the `appSecurity-2.0` and `ejbRemote-3.2` features are configured in the `server.xml` file.

### Before you begin

Understand the CSIV2 concepts, see [Common Secure Interoperability version 2 \(CSIV2\)](#) for further information.

### About this task

The following layers of security are available for inbound requests:

#### Procedure

1. Configure the inbound CSIV2 attribute layer.
2. Configure the inbound CSIV2 authentication layer.
3. Configure the inbound CSIV2 transport layer.

### Configuring inbound CSIV2 attribute layer



8.5.5.6

You can configure a Liberty server to claim support for identity assertion for inbound CSIV2 requests.

### About this task

The inbound CSIV2 attribute layer for a Liberty server has identity assertion that is disabled by default. The server supports Anonymous, Principal Name, X509 Certificate Chain, and Distinguished Name identity assertions from an upstream server that is acting as a client after the identity assertion is enabled through the `identityAssertionEnabled` attribute. You can use the `identityAssertionTypes` attribute to

specify the identity token types that the server supports. The `trustedIdentities` attribute can be used to specify the identity of the trusted upstream servers that are able to assert an identity to this server.

#### CAUTION:

Ensure that only trusted entities communicate with the server if presumed trust is set.

#### Procedure

1. Add the `appSecurity-2.0` and `ejbRemote-3.2` features in the `server.xml` file.

```
<featureManager>
  <feature>appSecurity-2.0</feature>
  <feature>ejbRemote-3.2</feature>
</featureManager>
```

The following is the default configuration without having to specify it in the `server.xml` file.

```
<orb id="default0rb">
  <serverPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Required"/>
      <transportLayer/>
    </layers>
  </serverPolicy.csiv2>
  <clientPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Supported"/>
      <transportLayer/>
    </layers>
  </clientPolicy.csiv2>
</orb>
```

2. Optional: If you need to change the default inbound attribute layer configuration, then add an `<orb>` element in the `server.xml` file as follows or add the `attributeLayer` element to an existing one. Replace the sample values in the example with your values.

```
<orb id="default0rb">
  <serverPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="true"/>
    </layers>
  </serverPolicy.csiv2>
</orb>
```

**Note:** The ID value `default0rb` in the `<orb>` element is predefined and cannot be modified.

3. Set the `trustedIdentities` attribute by changing the example values to the `trustedIdentity` of each of the upstream servers. The pipe character (`|`) must be used to separate the values when there are more than one asserting client.

```
<attributeLayer identityAssertionEnabled="true" trustedIdentities="yourAssertingUpstreamServer|anotherAssertingUpstreamServer"/>
```

4. Alternative: Instead of setting a named value for the `trustedIdentities` in step 2, you can set the `trustedIdentities` attribute with the character (`*`) to indicate that the server supports presumed trust. With presumed trust, any upstream server is able to assert an identity and must be used only when the upstream servers can be limited to a set of trusted servers. Therefore, use this value with caution.

```
<attributeLayer identityAssertionEnabled="true" trustedIdentities="*/>
```

5. When an upstream server that sends a certificate chain is trusted, add the issuer distinguished name of the certificate chain to the `trustedIdentities` attribute. For example,

```
<attributeLayer identityAssertionEnabled="true" trustedIdentities="CN=localhost,0=ibm,C=us"/>
```

6. Optional: If you need to change the default identity assertion token types that are supported by the server, then add the `identityAssertionTypes` attribute to the `attributeLayer` element in the `server.xml` file and specify a comma-separated list of values. The valid values are `ITTAnonymous`, `ITTPrincipalName`, `ITTX509CertChain`, and `ITTDistinguishedName`. For example, you can configure the

server to support identity assertions with X509 Certificate Chains or Distinguished Names. Replace the sample values in the example with your values.

```
<orb id="defaultOrb">
  <serverPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="true" identityAssertionTypes="ITTX509CertChain, ITTDistinguish
    </layers>
  </serverPolicy.csiv2>
</orb>
```

**Note:** The upstream server identity is obtained from the security information that the server sent in either the authentication layer or the transport layer. The authentication layer identity takes precedence over the transport identity, and the transport identity is used if no security information is sent at the authentication layer. For sample syntax and more information about `authenticationLayer` and `transportLayer` elements, see [Configuring inbound CSiv2 authentication layer](#) and [Configuring inbound CSiv2 transport layer](#).

Omitting a layer uses the default values for that layer.

## Results

Your inbound CSiv2 attribute layer is now configured for identity assertion.

## Configuring inbound CSiv2 authentication layer



8.5.5.6

You can configure a Liberty server to use a specific authentication mechanism for inbound CSiv2 requests.

### About this task

The inbound CSiv2 authentication layer for a Liberty server is enabled with the support for the LTPA and GSSUP authentication mechanisms by default. The `establishTrustInClient` association option of the authentication layer is set to `Required` by default to indicate that the authentication mechanisms specified are required. When you are using the LTPA mechanism, ensure that the communicating Liberty servers and other servers share the same LTPA keys.

### Procedure

1. Add the `appSecurity-2.0` and `ejbRemote-3.2` features in the `server.xml` file.

```
<featureManager>
  <feature>appSecurity-2.0</feature>
  <feature>ejbRemote-3.2</feature>
</featureManager>
```

The following example shows the default configuration without having to specify it in the `server.xml` file.

```
<orb id="defaultOrb">
  <serverPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Required"/>
      <transportLayer/>
    </layers>
  </serverPolicy.csiv2>
  <clientPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Supported"/>
    </layers>
  </clientPolicy.csiv2>
</orb>
```

```

        <transportLayer/>
    </layers>
</clientPolicy.csiv2>
</orb>

```

- Optional: If you need to change the default inbound authentication layer configuration, then add an <orb> element in the server.xml file as follows or add the authenticationLayer element to an existing one. Replace the sample values in the example with your values.

```

<orb id="default0rb">
  <serverPolicy.csiv2>
    <layers>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Required"/>
    </layers>
  </serverPolicy.csiv2>
</orb>

```

**Note:** The ID value default0rb in the <orb> element is predefined and cannot be modified.

- Optional: Set the mechanisms attribute to LTPA or GSSUP to use either LTPA or GSSUP (user name and password) only as the authentication mechanism.

```

<authenticationLayer mechanisms="LTPA" establishTrustInClient="Supported"/>
or
<authenticationLayer mechanisms="GSSUP" establishTrustInClient="Supported"/>

```

- Optional: Set the establishTrustInClient attribute to Required, Supported, or Never to indicate that the server requires, supports (optional), or never claims authentication with the specified mechanisms.

#### Notes:

- When the establishTrustInClient attribute is set to Required, only clients that either require or support compatible (at least one) authentication mechanisms are able to send a security context to the server.
- When the establishTrustInClient attribute is set to Supported, a client might choose whether to send the authentication information in the authentication layer.
- When the establishTrustInClient attribute is set to Never, the inbound CSIV2 authentication layer is disabled and at least one other CSIV2 layer must be enabled to authenticate.

Omitting a layer uses the default values for that layer.

For more information about the attributeLayer and transportLayer elements, see [Configuring inbound CSIV2 attribute layer](#) and [Configuring inbound CSIV2 transport layer](#).

## Results

Your inbound CSIV2 authentication layer is now configured.

## Configuring inbound CSIV2 transport layer



8.5.5.6

You can configure a Liberty server to claim support for client certificate authentication for inbound CSIV2 requests.

### About this task

The inbound CSIV2 transport layer for a Liberty server has client certificate authentication that is disabled by default. You can configure the transportLayer to specify the SSL configuration to use. You can configure the SSL element to either support or require the client certificate authentication. The certificate that is received is authenticated against the server user registry, and its identity is only used if no other form of authentication was sent in the CSIV2 request, like an identity assertion in the attribute layer or an authentication token in the authentication layer.

When you use the client certificate authentication, ensure that SSL is supported by the server.

## Procedure

1. Add the appSecurity-2.0 and ejbRemote-3.2 features in the server.xml file.

```
<featureManager>
  <feature>appSecurity-2.0</feature>
  <feature>ejbRemote-3.2</feature>
</featureManager>
```

The following example is the default configuration without having to specify it in the server.xml file.

```
<orb id="default0rb">
  <serverPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Required"/>
      <transportLayer/>
    </layers>
  </serverPolicy.csiv2>
  <clientPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Supported"/>
      <transportLayer/>
    </layers>
  </clientPolicy.csiv2>
</orb>
```

2. Configure SSL support as described in the “Enabling SSL communication in Liberty” on page 1834 page.
3. Configure the SSL element to use clientAuthentication or clientAuthenticationSupported. For example,

```
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore"
  trustStoreRef="defaultTrustStore" clientAuthentication="true" />
```

or

```
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore"
  trustStoreRef="defaultTrustStore" clientAuthenticationSupported="true" />
```

- If you specify clientAuthentication="true", then the server requests that a client sends a certificate. However, if the client does not have a certificate or if the certificate is not trusted by the server, then the handshake does not succeed.
  - If you specify clientAuthenticationSupported="true", then the server requests that a client sends a certificate. However, if the client does not have a certificate or if the certificate is not trusted by the server, then the handshake might still succeed.
  - If you do not specify either clientAuthentication or clientAuthenticationSupported, or if you specify clientAuthentication="false" or clientAuthenticationSupported="false", then the server does not request the client to send a certificate during the handshake.
4. Optional: If you need to change the default inbound transport layer configuration, then add an <orb> element in the server.xml file as follows or add the transportLayer element to an existing one. Replace the sample values in the example with your values.

```
<orb id="default0rb">
  <serverPolicy.csiv2>
    <layers>
      <transportLayer sslRef="defaultSSLConfig"/>
    </layers>
  </serverPolicy.csiv2>
</orb>
```

**Note:** The ID value default0rb in the <orb> element is predefined and cannot be modified.

5. Make sure the server trusts any client certificates that are used.

6. Make sure any client certificates that are used for client authentication are mapped to a user identity in your registry.
  - For the basic registry, the user identity is the common name (CN) from the distinguished name (DN) of the certificate.
  - For a Lightweight Directory Access Protocol (LDAP) registry, the DN from the client certificate must be in the LDAP registry.

Omitting a layer uses the default values for that layer. For more information about `attributeLayer` and `authenticationLayer` elements, see [Configuring inbound CSIV2 attribute layer](#) and [Configuring inbound CSIV2 authentication layer](#).

## Results

Your inbound CSIV2 transport layer is now configured for client certificate authentication.

## Configuring outbound CSIV2 in Liberty



8.5.5.6

The Common Secure Interoperability, version 2 (CSIV2) feature outbound configuration determines the type of authentication information sent for outbound requests. The CSIV2 feature is enabled automatically when the `appSecurity-2.0` and `ejbRemote-3.2` features are configured in the `server.xml` file.

### Before you begin

Understand the CSIV2 concepts, see [Common Secure Interoperability version 2 \(CSIV2\)](#) for further information.

### About this task

The following layers of security are available for outbound requests:

#### Procedure

1. Configure the outbound CSIV2 attribute layer.
2. Configure the outbound CSIV2 authentication layer.
3. Configure the outbound CSIV2 transport layer.

### Configuring outbound CSIV2 attribute layer



8.5.5.6

You can configure a Liberty server to perform identity assertions for outbound CSIV2 requests.

### About this task

Identity assertion is disabled by default in the outbound CSIV2 attribute layer for a Liberty server. The server that is acting as a client supports sending the Principal Name and Anonymous identity assertions to a downstream server after the identity assertion is enabled through the `identityAssertionEnabled` attribute. You can use the `identityAssertionTypes` attribute to specify more or different identity token types that the server supports for outbound requests. The `trustedIdentity` and `trustedPassword` attributes can be used to specify the identity of the client to be verified for trust by the downstream server when the authentication layer mechanism is GSSUP. The `trustedIdentity` attribute can be set without a `trustedPassword` if the authentication mechanism in the authentication layer is LTPA. You must also configure the upstream server along with enabling the identity assertion so that the client can assert an identity.

## Procedure

1. Add the appSecurity-2.0 and ejbRemote-3.2 features in the server.xml file.

```
<featureManager>
  <feature>appSecurity-2.0</feature>
  <feature>ejbRemote-3.2</feature>
</featureManager>
```

The following example is the default configuration without having to specify it in the server.xml file.

```
<orb id="default0rb">
  <serverPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Required"/>
      <transportLayer/>
    </layers>
  </serverPolicy.csiv2>
  <clientPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Supported"/>
      <transportLayer/>
    </layers>
  </clientPolicy.csiv2>
</orb>
```

2. Optional: If you need to change the default outbound attribute layer configuration, then add an <orb> element in the server.xml file as follows or add the attributeLayer element to an existing one. Replace the sample values in the example with your values.

```
<orb id="default0rb">
  <clientPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="true"/>
    </layers>
  </clientPolicy.csiv2>
</orb>
```

**Note:** The ID value default0rb in the <orb> element is predefined and cannot be modified.

3. Specify the upstream server identity for trust validation by the downstream server. The trustedIdentity specified must exist in the user registry of the target server.
  - When you are using the GSSUP mechanism in the authentication layer, you must set the trustedIdentity and trustedPassword attributes by changing the example values to the identity and password of the upstream server that is acting as a client.

```
<attributeLayer identityAssertionEnabled="true" trustedIdentity="yourTrustedId" trustedPassword="yourTrustedIdPwd"/>
```

Encode the password within the configuration. You can get the encoded value by using the securityUtility encode command.

- When you are using the LTPA mechanism in the authentication layer, you must set the trustedIdentity attribute by changing the example value to the identity of the upstream server that is acting as a client.

```
<attributeLayer identityAssertionEnabled="true" trustedIdentity="yourTrustedId"/>
```

4. Optional: If you need to change the default identity assertion token types that are supported by the server, then add the identityAssertionTypes attribute to the attributeLayer element in the server.xml file and specify a comma-separated list of values. The valid values are ITTAnonymous, ITTPrincipalName, ITTX509CertChain, andITTDistinguishedName. For example, you can configure the server to support identity assertions with X509 Certificate Chains or Distinguished Names. Replace the sample values in the example with your values.

```
<orb id="default0rb">
  <clientPolicy.csiv2>
    <layers>
```

```

        <attributeLayer identityAssertionEnabled="true" identityAssertionTypes="ITTX509CertChain, ITTDistingu
    </layers>
</clientPolicy.csiv2>
</orb>

```

#### Notes:

- If both LTPA and GSSUP are configured in the authentication layer and the downstream server supports LTPA, then LTPA takes precedence over GSSUP.
- If both LTPA and GSSUP are configured in the authentication layer and the downstream server supports only GSSUP, then GSSUP is used and the `trustedIdentity` and `trustedPassword` attributes must be specified.
- The `trustedIdentity` attribute is not required if you are using the transport certificate chain to identify the server to the downstream server. (The `identityAssertionEnabled` attribute is set to `true` and `establishTrustInClient` is set to `Never` in the `authenticationLayer`).
- Omitting a layer uses the default values for that layer.

For more information about `authenticationLayer` and `transportLayer` elements, see [Configuring outbound CSiv2 authentication layer](#) and [Configuring outbound CSiv2 transport layer](#).

## Results

Your outbound CSiv2 attribute layer is now configured for identity assertion.

## Configuring outbound CSiv2 authentication layer



8.5.5.6

You can configure a Liberty server to use specific authentication mechanisms for outbound CSiv2 requests.

### About this task

The outbound CSiv2 authentication layer for a Liberty server is enabled with support for the LTPA and GSSUP authentication mechanisms by default. The `establishTrustInClient` association option of the authentication layer is set to `Supported` by default to indicate that the authentication mechanisms specified are supported and optional.

When the LTPA mechanism is used, ensure that the communicating Liberty servers and other servers share the same LTPA keys.

### Procedure

1. Add the `appSecurity-2.0` and `ejbRemote-3.2` features in the `server.xml` file.

```

<featureManager>
  <feature>appSecurity-2.0</feature>
  <feature>ejbRemote-3.2</feature>
</featureManager>

```

The following example is the default configuration without having to specify it in the `server.xml` file.

```

<orb id="default0rb">
  <serverPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Required"/>
      <transportLayer/>
    </layers>
  </serverPolicy.csiv2>
</clientPolicy.csiv2>
  <layers>
    <attributeLayer identityAssertionEnabled="false"/>

```

```

        <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Supported"/>
        <transportLayer/>
    </layers>
</clientPolicy.csiv2>
</orb>

```

- Optional: If you need to change the default outbound authentication layer configuration, then add an <orb> element in the server.xml file as follows or add the authenticationLayer element to an existing one. Replace the sample values in the example with your values.

```

<orb id="default0rb">
  <clientPolicy.csiv2>
    <layers>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Supported"/>
    </layers>
  </clientPolicy.csiv2>
</orb>

```

**Note:** The ID value default0rb in the <orb> element is predefined and cannot be modified.

- Optional: Set the mechanisms attribute to LTPA or GSSUP to use either LTPA or GSSUP (user name and password) only as the authentication mechanism.

```
<authenticationLayer mechanisms="LTPA" establishTrustInClient="Supported"/>
```

or

```
<authenticationLayer mechanisms="GSSUP" establishTrustInClient="Supported"/>
```

- Optional: Set the establishTrustInClient attribute to Required, Supported, or Never to indicate that the server that is acting as a client requires, supports(optional), or never performs authentication with the specified mechanisms.

#### Notes:

- When the establishTrustInClient attribute is set to Required, the client is able to send an authentication token of one of the specified mechanisms only to servers that either require or support the same authentication mechanisms.
- When the establishTrustInClient attribute is set to Supported, the client might choose whether to send the authentication information in the authentication layer. If the downstream server is configured with Supported or Required, then the client sends a compatible authentication token.
- When the establishTrustInClient attribute is set to Never, the outbound CSiv2 authentication layer is disabled and at least one other CSiv2 layer must be enabled to authenticate to the downstream server.
- Omitting a layer uses the default values for that layer.

For more information about the attributeLayer and transportLayer elements, see [Configuring outbound CSiv2 attribute layer](#) and [Configuring outbound CSiv2 transport layer](#). For an example of a programmatic login when using GSSUP as the authentication mechanism, see [Example: Using the WSLogin configuration to create a basic authentication subject](#).

## Results

Your outbound CSiv2 authentication layer is now configured.

## Configuring outbound CSiv2 transport layer



8.5.5.6

You can configure a Liberty server to perform client certificate authentication for outbound CSiv2 requests.

## About this task

The client certificate authentication of the outbound CSiv2 transport layer for a Liberty server is disabled by default. You can configure the transportLayer to specify the SSL configuration to use.

You can configure the SSL element to support client certificate authentication or require it. The certificate sent to the downstream server is authenticated against the downstream server user registry and its identity is only used if no other form of authentication is sent in the CSiv2 request, like an identity assertion in the attribute layer or an authentication token in the authentication layer.

When the client certificate authentication is used, ensure that SSL is supported by this server.

## Procedure

1. Add the appSecurity-2.0 and ejbRemote-3.2 features in the server.xml file.

```
<featureManager>
  <feature>appSecurity-2.0</feature>
  <feature>ejbRemote-3.2</feature>
</featureManager>
```

The following example is the default configuration without having to specify it in the server.xml file.

```
<orb id="defaultOrb">
  <serverPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Required"/>
      <transportLayer/>
    </layers>
  </serverPolicy.csiv2>
  <clientPolicy.csiv2>
    <layers>
      <attributeLayer identityAssertionEnabled="false"/>
      <authenticationLayer mechanisms="LTPA,GSSUP" establishTrustInClient="Supported"/>
      <transportLayer/>
    </layers>
  </clientPolicy.csiv2>
</orb>
```

2. Configure SSL support as described in Enabling SSL communication for Liberty.
3. Optional: Configure the SSL element to use clientAuthentication or clientAuthenticationSupported. For example,

```
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore"
  trustStoreRef="defaultTrustStore" clientAuthentication="true" />
```

or

```
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore"
  trustStoreRef="defaultTrustStore" clientAuthenticationSupported="true" />
```

4. Optional: If you need to change the default outbound transport layer configuration, then add an <orb> element in the server.xml file as follows or add the transportLayer element to an existing one. Replace the sample values in the example with your values.

```
<orb id="defaultOrb">
  <clientPolicy.csiv2>
    <layers>
      <transportLayer sslRef="defaultSSLConfig"/>
    </layers>
  </clientPolicy.csiv2>
</orb>
```

**Note:** The id value *defaultOrb* in the <orb> element is predefined and cannot be modified.

5. Make sure the downstream server trusts any client certificates that are sent from this server.

6. Make sure that any client certificates used for client authentication are mapped to a user identity in the downstream server user registry.
  - For the basic registry, the user identity is the common name (CN) from the distinguished name (DN) of the certificate.
  - For a Lightweight Directory Access Protocol (LDAP) registry, the DN from the client certificate must be in the LDAP registry.

**Notes:**

- When the `clientAuthentication` attribute is set to `true` in the `<ssl>` element, the client sends a client certificate only to servers that either require or support the client certificate authentication.
- When the `clientAuthenticationSupported` attribute is set to `true` in the `<ssl>` element, the client might choose whether to send a client certificate based on the `<ssl>` element configuration that is used by the downstream server.
- When the `clientAuthentication` and `clientAuthenticationSupported` attributes are not set in the `<ssl>` element, then the server that is acting as a client is not enabled with the client certificate authentication.

Omitting a layer uses the default values for that layer. For more information about the `attributeLayer` and `authenticationLayer` elements, see [Configuring outbound CSIV2 attribute layer](#) and [Configuring outbound CSIV2 authentication layer](#).

## Results

Your outbound CSIV2 transport layer is now configured for client certificate authentication.

---

## Configuring security for the Liberty application client container and its applications



8.5.5.6

Configure security on the Liberty application client container and its applications to ensure communications between the client and server are secure. You can also configure security to ensure that credentials of clients flow to the server.

### Enabling SSL communication for the Liberty application client container



8.5.5.6

The Liberty application client container might require some SSL configuration for the client container to communicate with a server. Configuring SSL for the application client container requires the use of the same SSL feature, `ssl-1.0`, that the server requires for SSL enablement. The configuration elements and attributes are the same for the application client as for the server; however, for the application client container, these values are specified in the `client.xml` file.

### About this task

The SSL handshake is a series of messages that are exchanged over the SSL protocol between a client and a server to negotiate for connection-specific protection. To enable SSL for the Liberty application client container the SSL feature, `ssl-1.0`, must include the minimal information that is needed to form an SSL configuration that is used by the client. The minimal information that is required to form an SSL configuration is a keystore and a password.

You can use the securityUtility **createSSLCertificatecommand** to create the keystore of the client and to provide you with information about the configuration. Using the tool is optional, because you can also create a keystore and the associated configuration for other customer-defined purposes.

## Procedure

Add the keystore element to the `client.xml` file. The `id` attribute must be `defaultKeyStore` and the `password` attribute contains the keystore password. The password can be entered in clear text or encoded. Use the securityUtility `encode` option to encode the password.

```
<keyStore id="defaultKeyStore" password="yourPassword" />
```

This is the minimum configuration that is needed to create an SSL configuration. In this configuration, the client creates the keystore and certificate if it does not exist during SSL initialization. The password that is provided must be at least 6 characters long. JKS is the default keystore type and the default keystore is called `key.jks` and these defaults are in the `<client home>/resources/security` directory. The client will create the `defaultKeyStore` the first time it starts when using the previous configuration, however having the client create the default certificate comes with a performance cost. To avoid the performance cost it is recommended that the **securityUtility createSSLCertificate** command be used to create the default keystore used in the `defaultKeyStore` configuration. If you need a custom SSL configuration, see SSL configuration attributes.

### Accepting signer certificates

If the client does not have an established trust relationship with the server the communication with the client prompts the user and asks if they accept the certificate from the server. If the user responds with yes, the certificate is taken and stored in the client keystore configuration and the command proceeds. If the user specifies no then there is no trust that is established and the call ends in an error.

Example of what the prompt looks like:

```
*** SSL SIGNER EXCHANGE PROMPT ***
```

```
The SSL signer from target host is not found in trust store C:/liberty/workspace/build.image/wlp/usr/clients/myT
```

Here is the signer information (verify the digest value matches what is displayed at the server):

```
Subject DN: CN=localhost, O=ibm, C=us
Issuer DN: CN=localhost, O=ibm, C=us
Serial number: 1327582458
Expires: Sun Jan 04 06:54:18 CST 2099
SHA-1 Digest: 00:6F:25:F1:78:5D:EB:00:B1:E2:99:DB:E8:D7:DF:3B:F8:E0:20:9A
Add signer to the trust store now? (y/n)
```

You might receive the following error message if the user specifies no when asked to add the signer to the truststore:

```
[ERROR ] CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN CN=localhost, O=ibm, C=us
sent from the target host. The signer might need to be added to local trust store C:/liberty/workspace/build.im
    java.security.cert.CertPathValidatorException: The certificate issued by SubjectDN CN=localhost, O=ibm, C
    java.security.cert.CertPathValidatorException: Certificate chaining error
throw able: javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: PKIX path building fai
: PKIXCertPathBuilderImpl could not build a valid CertPath.; internal cause is:

    java.security.cert.CertPathValidatorException: The certificate issued by
SubjectDN CN=localhost, O=ibm, C=us is not trusted; internal cause is:
    java.security.cert.CertPathValidatorException: Certificate chaining error
```

### Auto accept signer certificate

If the client does not want to be prompted for the signer certificate and chooses to accept the server signer certificate without examining the certificate, the user can provide the `-autoAcceptSigner` flag to the client container command line.

```
client run client_name --autoAcceptSigner
```

### Client authentication

If the client is communicating with a server that has client authentication that is enabled, then the

server needs to trust the client as well as the client trusting the server. The client must have a key, and personal certificate, in its keystore. If you use the `securityUtility createSSLCertificate` command, the keystore contains a personal certificate. The server that the client application container is communicating with must trust the client, so the signer from the client needs to be added to the truststore of the server. You can use the `java` tool, `keytool`, to extract the signer from the keystore of the application client container and add the certificate from the client to the truststore of the server.

## Configuring a JAAS programmatic login on the Liberty application client container



8.5.5.6

The Liberty application client container can be configured to use a JAAS programmatic login.

### Before you begin

Review the different ways of authenticating users on the application client container, and decide whether the programmatic login option is best for your environment. For further details, see [Authentication on the Liberty application client container](#).

### About this task

A programmatic login is a type of form login that supports application presentation login forms for authentication. This approach requires the application developer to collect the user's credentials and authenticate that user. This method takes advantage of the JAAS framework to send a user's credentials to the server for authentication. The JAAS framework consists of creating a login context by specifying a JAAS login configuration and by using a callback handler to gather the user's credentials. When a subject is obtained from the login context, you can use a Liberty security API to set that Subject on the thread, and it is used for your outbound call to the server.

The JAAS login configuration specifies how and which login modules are used for authentication. Here are the JAAS login configurations that are provided by Liberty on the client:

- **WSLogin JAAS login configuration:** A generic JAAS login configuration that a Liberty application client container application can use to perform authentication that is based on a user ID and password. However, this configuration does not support the `CallbackHandler` handler that is specified in the deployment descriptor of the client application module.
- **ClientContainer JAAS login configuration:** This JAAS login configuration recognizes the `CallbackHandler` handler that is specified in the client application module's deployment descriptor, if one is specified. If a handler is not specified in the deployment descriptor, then the handler that was specified programmatically is used.

The login modules that are specified by the JAAS login configuration implement a certain authentication technology. A login module can gather credentials from the user by using the `javax.security.auth.callback.CallbackHandler` interface. Liberty provides a non-prompt implementation of the `CallbackHandler` interface, which is called `com.ibm.websphere.security.auth.callback.WSCallbackHandlerImpl`. This implementation enables an application developer to specify the credentials directly in the application without having to prompt the user. There are two ways to specify your `CallbackHandler` implementation:

- Specify your implementation programmatically, as an argument to the `javax.security.auth.login.LoginContext` constructor; for example:

```
LoginContext logincontext = new LoginContext("ClientContainer", new WSCallbackHandlerImpl("user", "password"));
```
- Specify your implementation name in the client application module's deployment descriptor (`application-client.xml`); for example:

```
<callbackhandler>com.acme.callbackhandler.WSCallbackHandlerImpl</callbackhandler>
```

**Note:** The WSLgin login configuration does not recognize the second option of specifying a CallbackHandler handler in the deployment descriptor.

## Procedure

1. Add the appSecurityClient-1.0 feature to your client.xml file.  

```
<feature>appSecurityClient-1.0</feature>
```
2. Configure SSL for your client:
  - a. **Optional:** Use the **securityUtility** command to create an SSL certificate for the client; for example:  

```
securityUtility createSSLCertificate --client=myClient --password=liberty
```
  - b. **Recommended:** Use the **securityUtility** command to generate an xor encoded password. For example, to encode the password liberty:  

```
securityUtility encode liberty
```
  - c. Add a keyStore element to your client.xml file. The following example uses the default SSL configuration:  

```
<keyStore id="defaultKeyStore" password="{xor}MzY90i0rJg==" /> <!-- pwd: liberty -->
```
3. In the application code, create a Subject using the ClientContainer JAAS login configuration and the WSCallbackHandlerImpl callback handler.
  - a. Before the application makes an outbound request, add the following code. Change the userName and userPassword to valid credentials for a user that exists in the user registry of the target server.

```
CallbackHandler wscbh = new WSCallbackHandlerImpl("userName", "userPassword");
LoginContext ctx = null;
try {
    ctx = new LoginContext("ClientContainer", wscbh);
} catch (LoginException le) {
    le.printStackTrace();
}
try {
    ctx.login();
} catch (LoginException le) {
    le.printStackTrace();
}
Subject subject = ctx.getSubject();
```
4. Set the Subject obtained in the previous step on the thread and use that Subject to look up an EJB. Use the WSSubject.doAs, or doAsPrivileged APIs to accomplish this action. The Subject within the com.ibm.websphere.security.auth.WSSubject.doAs or com.ibm.websphere.security.auth.WSSubject.doAsPrivileged code block is used for Java Platform, Enterprise Edition (J2EE) resources authorization checks.

```
WSSubject.doAs(subject, new PrivilegedAction() {
    public Object run() {
        try {
            //Perform EJB lookup and invocation
        } catch (Exception ex) {
            ex.printStackTrace();
        }
        return null;
    }
});
```
5. 8.5.5.7 If Java 2 security is enabled on your client and your application code is calling JAAS or Liberty security APIs, add the necessary Java 2 Security permissions to either the permissions.xml file or the client.xml file of the application. For more details on which Liberty security APIs are protected by Java 2 Security permissions, see Programming Interfaces (APIs). For further details, see Java 2 Security.

## What to do next

As on the server, you can use a custom login module to either make more authentication decisions or add information to the subject to make finer-grained authorization decisions inside your client application. For further details, see [Configuring a JAAS custom login module for the Liberty application client container](#).

## Configuring a JAAS custom login module for the Liberty application client container



8.5.5.6

You can configure the Liberty application client container to use a custom Java Authentication and Authorization Service (JAAS) login module.

### Before you begin

Make sure that you have a JAR file that contains the JAAS custom login module, which implements the `javax.security.auth.spi.LoginModule` interface.

### About this task

You can use a custom login module to either make additional authentication decisions or add information to the subject to make finer-grained authorization decisions inside your application. To configure a JAAS custom login module, complete the following steps.

### Procedure

1. Add the `appSecurityClient-1.0` feature to your `client.xml` file.  

```
<feature>appSecurityClient-1.0</feature>
```
2. Create a class `com.sample.CustomLoginModule` that implements the `LoginModule` interface and package it into the `CustomLoginModule.jar` file.
3. Create a `<library>` element that uses a `<fileset>` element that indicates where the `CustomLoginModule.jar` file is. In this example, the file is in the client's configuration directory, and the library id is `customLoginLib`.

```
<library id="customLoginLib">  
  <fileset dir="{server.config.dir}" includes="CustomLoginModule.jar"/>  
</library>
```

4. Create a `<jaasLoginModule>` element. In this example, the id is `myCustom`.
  - a. Configure the custom login module to require a successful authentication by setting the `controlFlag` attribute to `REQUIRED`.
  - b. Set the `libraryRef` attribute to `customLoginLib`, the id of the `<library>` element that is configured in the previous step.

```
<jaasLoginModule id="myCustom" className="com.sample.CustomLoginModule" controlFlag="REQUIRED" libraryRef="customLO
```

5. Create a `<jaasLoginContextEntry>` element with the id and name of the system-defined JAAS configuration on the application client container: `ClientContainer`. You can also set this JAAS configuration to `WSLogin`, or your own JAAS configuration. In the `loginModuleRef` attribute, add `proxy`, the id for the proxy login module and `myCustom`, the id of the `jaasLoginModule` element that is created in the previous step.

```
<jaasLoginContextEntry id="ClientContainer" name="ClientContainer"  
  loginModuleRef="proxy, myCustom"/>
```

# Configuring Common Secure Interoperability version 2 (CSiv2) in the Liberty application client container



8.5.5.6

The WebSphere Application Server Liberty application client container supports CSiv2 security at various levels such as the message authentication (message layer), and client certificate authentication (transport layer). Using the CSiv2 feature, you can specify the type of authentication for outbound requests to the servers. CSiv2 features are enabled by default. You can configure CSiv2 in the Liberty application client container to enable interoperability between Java Platform, Enterprise Edition vendors.

## Configuring outbound CSiv2 in the Liberty application client container



8.5.5.6

CSiv2 features are enabled by default. You can configure CSiv2 in the Liberty application client container to enable interoperability between Java Platform, Enterprise Edition vendors.

### Before you begin

Understand the CSiv2 concepts, see Common Secure Interoperability version 2 (CSiv2) for further information.

### Configuring the outbound CSiv2 authentication layer in the Liberty application client container:

8.5.5.6

You can configure a Liberty application client container to use specific authentication mechanisms for outbound CSiv2 requests.

### About this task

The outbound CSiv2 authentication layer for a Liberty application client container is enabled with support for the GSSUP authentication mechanism by default. The `establishTrustInClient` association option of the authentication layer is set to `Supported` by default to indicate that the authentication mechanisms specified are supported and optional.

### Procedure

1. Configure the `orb` element in the `client.xml` file as follows or add the `authenticationLayer` element to an existing one, replacing the sample values in the example with your values:

```
<orb id="default0rb">
  <clientPolicy.clientContainerCsiv2>
    <layers>
      <authenticationLayer user="userId" password="{xor}PDC+MTg6Ejo="/>
    </layers>
  </clientPolicy.clientContainerCsiv2>
</orb>
```

**Note:** The `id` value `default0rb` in the `orb` element is predefined and cannot be modified.

**Note:** Hash encoding cannot be used for encrypting the password because the original password cannot be decoded from the hashed value.

The `mechanisms` and `establishTrustInClient` attributes are optional. The only supported value, and the default value, for the `mechanisms` attribute is `GSSUP`.

Without specifying an `<orb>` element, the following configuration is implicit.

```

<orb id="defaultOrb">
  <clientPolicy.clientContainerCsiv2>
    <layers>
      <authenticationLayer mechanisms="GSSUP" establishTrustInClient="Supported"/>
      <transportLayer/>
    </layers>
  </clientPolicy.clientContainerCsiv2>
</orb>

```

2. **Optional:** Set the user and password attributes with a valid user ID and password to access the server. By default, a server requires the GSSUP mechanism for inbound connections, meaning that the server must receive a user and password and because of this requirement, the user, and password values are required in the client.xml file, unless a programmatic login is implemented by the application.
3. **Optional:** Set the establishTrustInClient attribute to Required, Supported (default), or Never for performing authentication with the specified mechanisms. For example,

```

<orb id="defaultOrb">
  <clientPolicy.clientContainerCsiv2>
    <layers>
      <authenticationLayer user="userId" password="{xor}PDC+MTg6Ejo=" establishTrustInClient="Required" />
    </layers>
  </clientPolicy.clientContainerCsiv2>
</orb>

```

**Note:**

- When the establishTrustInClient attribute is set to Required, the client is able to send an authentication token of one of the specified mechanisms only to servers that either require or support the same authentication mechanisms.
- When the establishTrustInClient attribute is set to Supported (default), the client can choose whether to send the authentication information in the authentication layer. If the server is configured with Supported or Required of the same authentication mechanisms, then the client sends a compatible authentication token.
- When the establishTrustInClient attribute is set to Never, the outbound CSiv2 authentication layer is disabled and the CSiv2 transport layer must be enabled to authenticate to the server.

**Results**

Your outbound CSiv2 authentication layer is now configured.

**Configuring the outbound CSiv2 transport layer in the Liberty application client container:** 

8.5.5.6

You can configure the Liberty application client container to perform client certificate authentication for outbound CSiv2 requests.

**About this task**

The client certificate authentication of the outbound CSiv2 transport layer for a Liberty application client container is not used by default. You can configure the transportLayer to specify the SSL configuration to use.

You can configure the SSL element to support client certificate authentication or require it. The certificate sent to the server is authenticated against the server user registry and its identity is only used if no other form of authentication is sent in the CSiv2 request, like an identity assertion in the attribute layer or an authentication token in the authentication layer.

## Procedure

1. Configure SSL support as described in Enabling SSL communication for the Liberty application client container.
2. Optional: Configure the SSL element to use `clientAuthentication` or `clientAuthenticationSupported`. For example,

```
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore"
    trustStoreRef="defaultTrustStore" clientAuthentication="true" />
```

or

```
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore"
    trustStoreRef="defaultTrustStore" clientAuthenticationSupported="true" />
```

3. Configure the `<orb>` element in the `client.xml` file as follows or add the `transportLayer` element to an existing one and replace the sample values in the sample with your values:

```
<orb id="defaultOrb">
  <clientPolicy.clientContainerCsi2>
    <layers>
      <transportLayer sslRef="defaultSSLConfig"/>
    </layers>
  </clientPolicy.clientContainerCsi2>
</orb>
```

Without specifying an `<orb>` element, the following configuration is implicit.

```
<orb id="defaultOrb">
  <clientPolicy.clientContainerCsi2>
    <layers>
      <authenticationLayer mechanisms="GSSUP" establishTrustInClient="Supported"/>
      <transportLayer/>
    </layers>
  </clientPolicy.clientContainerCsi2>
</orb>
```

4. Make sure the server trusts any client certificates that are sent from this server.
  - When the `clientAuthentication` attribute is set to `true` in the `ssl` element, the client sends a client certificate only to servers that either require or support the client certificate authentication.
  - When the `clientAuthenticationSupported` attribute is set to `true` in the `ssl` element, the client might choose whether to send a client certificate based on the `ssl` element configuration used by the server.
  - When the `clientAuthentication` and `clientAuthenticationSupported` attributes are not set in the `ssl` element, the server that is acting as a client is not enabled with the client certificate authentication.

## Results

Your outbound CSIv2 transport layer is now configured for client certificate authentication.

---

## Configuring Java Servlet 3.1 support for security



8.5.5.4

Liberty supports all security updates as defined in the Java Servlet 3.1 specification.

### About this task

Take advantage of the Java Servlet 3.1 features on Liberty.

## Procedure

1. Add the servlet-3.1 feature in the server.xml file:

```
<feature>servlet-3.1</feature>
```

2. Determine which of the following Java Servlet 3.1 functions that you want to use:

- Specify autocomplete=off in the login form.

When you use HTML for a form login page, set the password form field to autocomplete="off" to disable automatically filling in passwords in the web browser. For example:

```
<form method="POST" action="j_security_check">
<input type="text" name="j_username">
<input type="password" name="j_password" autocomplete="off">
</form>
```

- Specify the all authenticate security constraint (\*\*).

The special role name \*\* indicates any authenticated user. When \*\* displays in an authorization constraint, if the user is authenticated, that user has access to the methods that are specified in the constraint. Users do not have to be mapped to this role in the application bindings. For example:

```
<security-constraint id="SecurityConstraint_1">
  <web-resource-collection id="WebResourceCollection_1">
    <web-resource-name>Protected with ** role</web-resource-name>
    <url-pattern>/AnyAuthSecurityConstraint</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint id="AuthConstraint_1">
    <role-name>**</role-name>
  </auth-constraint>
</security-constraint>
```

When the isUserInRole() method is called with a role name of \*\*, isUserInRole() returns true if the user is authenticated. If \*\* is a defined role in the configuration in a security-role, it is not treated like the special any authenticated user role. The user must be mapped to that role in application bindings for isUserInRole to return true.

- Specify the deny-uncovered-http-methods flag in web.xml files.

If the deny-uncovered-http-methods element is specified within the web.xml file, the container denies any uncovered HTTP methods that are not enumerated within the combined security constraint for a URL pattern that is the best match for the request URL. A 403 (SC\_FORBIDDEN) status code is returned. For example:

```
<servlet-mapping id="ServletMapping_1">
  <servlet-name>MyServlet</servlet-name>
  <url-pattern>/MyURLPattern</url-pattern>
</servlet-mapping>
```

```
<deny-uncovered-http-methods/>
```

```
<!-- SECURITY CONSTRAINTS -->
```

```
<security-constraint id="SecurityConstraint_1">
  <web-resource-collection id="WebResourceCollection_1">
    <web-resource-name>Protected with Employee or Manager roles</web-resource-name>
    <url-pattern>/MyURLPattern</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint id="AuthConstraint_1">
    <role-name>Employee</role-name>
    <role-name>Manager</role-name>
  </auth-constraint>
</security-constraint>
```

If the deny-uncovered-http-methods element is specified in the web.xml file, a message is logged in the messages.log file for each URL pattern in each servlet, indicating the uncovered methods with a note that those uncovered methods are unprotected and not accessible. For example:

For URL MyURLPattern in servlet MyServlet, the following HTTP methods are uncovered, and not accessible: DELETE OPTION  
If the deny-uncovered-http-methods element is not specified in the web.xml file, a message is logged in the messages.log file for each URL pattern in each servlet, indicating the uncovered methods with a note that those uncovered methods are unprotected and accessible. For example:

For URL MyURLPattern in servlet MyServlet, the following HTTP methods are uncovered, and accessible: DELETE OPTION

## Results

You have now secured your application.

---

## Configuring secure JMX connection to Liberty

You can access the secured Java Management Extensions (JMX) connectors on Liberty by using SSL. The secured JMX connection is enabled by the Liberty feature restConnector-1.0.

### About this task

The REST connector is enabled through the Liberty feature restConnector-1.0. Remote access through the REST connector is protected by a single administrator role. In addition, SSL is required to keep the communication confidential. The restConnector-1.0 feature already includes the ssl-1.0 feature.

**Note:** An application deployed on Liberty has unrestricted access to its MBeanServer directory.

The following section describes how to configure and access the REST connector on Liberty.

### Procedure

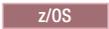
1. Enable the REST connector using the following code in the server.xml file.

```
<featureManager>  
  <feature>restConnector-1.0</feature>  
</featureManager>
```

2. Configure SSL certificates in the server.xml file.

Ensure that the CN value of the certificate's subjectDN is the host name of the machine where the server is running, and that the truststore contains the certificate of the server in the jConsole connection.

3. Configure a user or group to the administrator role in the server.xml file.

- Map to the administrator role for Liberty
-  Map to the administrator role for Liberty on z/OS

4. Access the REST connector.

 You can access a Liberty REST connector from a Java client or directly through an HTTPS call. A Java client uses the client-side of the connector, which is in wlp/clients/restConnector.jar and implements the javax.management.MBeanServerConnection interface. HTTPS calls use the server-side of the connector. As to HTTPS calls on the server-side, any programming language that can make HTTPS calls, such as C++, JavaScript, curl, Ruby, and Perl, can use the REST APIs. The REST APIs contain endpoints for management (JMX), file transfer, collective routing and collective deployment.

- Access the REST connector from a JMX client application or by using the jConsole tool provided in the Java SDK. Use -J flags to pass the system properties as Java options and set the class path to include the connector class files. The connector class files are packed in the clients/restConnector.jar file.

– Use the following properties for SSL certificates:

```
-J-Djavax.net.ssl.trustStore=<location of your client trust store>  
-J-Djavax.net.ssl.trustStorePassword=<password for the trust store>  
-J-Djavax.net.ssl.trustStoreType=<type of trust store>
```

The following example shows the jConsole tool being used with SSL configurations:

```
jconsole -J-Djava.class.path=%JAVA_HOME%/lib/jconsole.jar;  
          %JAVA_HOME%/lib/tools.jar;  
          %WLP_HOME%/clients/restConnector.jar  
-J-Djavax.net.ssl.trustStore=key.jks  
-J-Djavax.net.ssl.trustStorePassword=Liberty  
-J-Djavax.net.ssl.trustStoreType=jks
```

After the jConsole starts, select **Remote Process**, and enter the JMX service URL:  
service:jmx:rest://<host>:<port>/IBMJMXConnectorREST. The port number is the HTTPS port.  
You must also provide the user name and password.

- **z/OS** For z/OS, use the following system properties:

```
-J-Djava.protocol.handler.pkgs=com.ibm.crypto.provider  
-J-Djavax.net.ssl.trustStore=<SAF keyring>  
-J-Djavax.net.ssl.trustStorePassword=<password to SAF>  
-J-Djavax.net.ssl.trustStoreType=JCERACFKS
```

- **8.5.5.4** Access the REST connector directly using an HTTPS call.

To use HTTPS calls to access REST connectors, you need WebSphere Application Server Liberty 8.5.5.4 or later.

- a. Open a browser at `https://<host>:<port>/IBMJMXConnectorREST/api`, and enter the administrative credentials you specified in step 3.
- b. Examine the available REST APIs. Each item has a description of its behavior, input, output, query parameters, and header.

**Note:** You can specify some JMX REST connection options as system properties. See the Liberty API - WebSphere JMX REST Connector API.

---

## Configuring web security related properties in Liberty

You can configure web security related properties for Liberty, such as SSO and client certificate authentication.

### About this task

You can use the `webAppSecurity` element to configure web container application security for Liberty.

Make sure you add the `appSecurity-2.0` **8.5.5.0**, `servlet-3.0` and other required Liberty features to the `server.xml` file.

For all available attributes in the `webAppSecurity` element, see .

You can choose to complete one or more of the following tasks according to your requirements.

### Procedure

- “Customizing SSO configuration using LTPA cookies in Liberty” on page 1887
- “Configuring your web application and server for client certificate authentication” on page 1847

## Customizing SSO configuration using LTPA cookies in Liberty

With single sign-on (SSO) configuration support, web users can authenticate once when accessing Liberty resources such as HTML, JavaServer Pages (JSP) files, and servlets, or accessing resources in multiple Liberty servers that share the same Lightweight Third Party Authentication (LTPA) keys.

### Example

When a user passes authentication on one of Liberty servers, authentication information generated by the server is transported to the web browser in a cookie. The cookie is used to propagate the authentication information to other Liberty servers.

The LTPA is configured and ready for immediate use. The default cookie name used to store the SSO token is called `ltpaToken2`. If you want to use a different name for the cookie, you can customize the cookie name using the **ssoCookieName** attribute of the `<webAppSecurity>` element. If you customize the cookie name, make sure that all the servers that participate in SSO use the same cookie name.

For more information about SSO, see SSO concept in Liberty.

The following example code sets the user to be logged out after the HTTP session expires and the name of the SSO cookie as `myCookieName`:

```
<webAppSecurity logoutOnHttpSessionExpire="true" ssoCookieName="myCookieName" />
```

**Note:** For SSO to work across Liberty servers, full profile servers, or both, set the following resources:

- The servers must use the same LTPA keys and share the same user registry.
- If the servers are not in the same domain, use the **ssoDomainNames** attribute of the `<webAppSecurity>` element to list the domains. The following example code sets the domain name to `domain.com`:

```
<webAppSecurity ssoDomainNames="domain.com" />
```

- If the servers are in the same domain, set the **ssoUseDomainFromURL** attribute of the `<webAppSecurity>` element to `true`, or specify the domain name in the **ssoDomainNames** attribute. The following example code sets **ssoUseDomainFromURL** to `true` so that the domain name is taken from the request URL:

```
<webAppSecurity ssoUseDomainFromURL="true" />
```

For details of all the available SSO settings, see the `<webAppSecurity>` element in .

## Configuring your web application and server for client certificate authentication

You can configure your web application on Liberty using SSL client authentication.

### Before you begin

This topic assumes that you have already created the SSL certificates, for example as described in “Creating SSL certificates from the command line” on page 1844.

### About this task

Client certificate authentication occurs if the server-side requests that the client-side send a certificate. A WebSphere server can be configured for client certificate authentication on the SSL configuration. To do this, you add the `ssl-1.0` Liberty feature to the `server.xml` file, along with code that tells the server the keystore information for authentication.

For details of which aspects of SSL are supported, see “Liberty features” on page 826.

### Procedure

1. Ensure that the deployment descriptor for your web application specifies client certificate authentication as the authentication method to use.

Check that the deployment descriptor includes the following element:

```
<auth-method>CLIENT-CERT</auth-method>
```

**Note:** You can use a tool such as Rational Application Developer to create the deployment descriptor.

2. Optional: Generate an SSL certificate using the command line. See “Liberty:securityUtility command” on page 1844.
3. Configure your server to enable SSL client authentication by adding the following lines to the `server.xml` file:

```
<featureManager>
  <feature>ssl-1.0</feature>
</featureManager>
```

```
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore"
  trustStoreRef="defaultTrustStore" clientAuthenticationSupported="true" />
<keyStore id="defaultKeyStore" location="key.jks" type="JKS" password="defaultPWD" />
<keyStore id="defaultTrustStore" location="trust.jks" type="JKS" password="defaultPWD" />
```

- If you specify `clientAuthentication="true"`, the server requests that a client sends a certificate. However, if the client does not have a certificate, or the certificate is not trusted by the server, the handshake does not succeed.
  - If you specify `clientAuthenticationSupported="true"`, the server requests that a client sends a certificate. However, if the client does not have a certificate, or the certificate is not trusted by the server, the handshake might still succeed.
  - If you do not specify either `clientAuthentication` or `clientAuthenticationSupported`, or you specify `clientAuthentication="false"` or `clientAuthenticationSupported="false"`, the server does not request that a client send a certificate during the handshake.
4. Add a client certificate to your browser. See the documentation of your browser for adding client certificates.
  5. Make sure the server trusts any client certificates that are used.
  6. Make sure any client certificates used for client authentication are mapped to a user identity in your registry.
    - For the basic registry, the user identity is the common name (CN) from the distinguished name (DN) of the certificate.
    - For a Lightweight Directory Access Protocol (LDAP) registry, the DN from the client certificate must be in the LDAP registry.
  7. To use basic authentication, user ID and password only, if client certificate authentication does not succeed, add the following line to your `server.xml` file.

```
<webAppSecurity allowFailOverToBasicAuth="true" />
```

**Note:** If you specify `allowFailOverToBasicAuth="false"` or do not specify `allowFailOverToBasicAuth`, and the client certificate authentication does not succeed, the request generates a 403 Authentication error message, and the client is not prompted for basic authentication.

## Configuring the Liberty server to track logged out LTPA tokens

8.5.5.4

You can configure a Liberty server to track logged out Lightweight Third Party Authentication (LTPA) tokens.

### About this task

When a user is logged out by using either form logout or programmatic logout, the LTPA token that is used for Single Sign On is removed from the cookie. The LTPA token that is used for SSO is also removed from the local Authentication cache and the session is invalidated. If the token was persisted and presented again, it is validated based on the expiration time and the LTPA encryption keys.

With this element enabled, the LTPA SSO tokens that were logged out on the server are tracked and if presented again on the same server are not used.. A logout is performed and the user needs to authenticate again.

This configuration only works on the same server. This means that the LTPA token can only be tracked on the server where the user logged out, and if that same LTPA token is presented to another server it is

used and if the LTPA keys are shared and the token has not expired it is used until it is also logged out on that server.

## Procedure

To track the tokens that are logged out on a particular Liberty server, you can enable the following element in the `server.xml`:

```
<webAppSecurity trackLoggedOutSSOCookies="true"/>
```

When this element is enabled, it might affect your Single Sign On (SSO) scenarios. For example, if the user 'bob' logs in from multiple browsers to the same server and logs out from one browser and tries to access the resource by using another browser, the user must log in as the token presented is discarded.

---

## Configuring authentication aliases for Liberty

You can configure an authentication data alias to use with a resource reference for authentication in Liberty.

### About this task

You can use an authentication data alias by defining a user and password for authentication in Liberty. To do this, add the `jdbc-4.0` Liberty feature to the `server.xml` file and add at least one `authData` element.

**Note:** There is no authentication alias principal mapping module support.

## Procedure

1. Add the `jdbc-4.0` Liberty features in the `server.xml` file.

```
<featureManager>  
  <feature>jdbc-4.0</feature>  
</featureManager>
```

2. Configure the `authData` element in the `server.xml` file as follows. If the `authData` element is used as a top-level configuration element, you must set the `id` attribute value to a unique authentication alias.

```
<authData id="auth1" user="dbuser1" password="dbuser1pwd"/>
```

3. Configure the IBM deployment descriptor, for example, the `ibm-web-bnd.xml` file, of your application by using the `authentication-alias` element in the resource reference. The `name` attribute value must match the `id` attribute defined in the `server.xml` file.

```
<resource-ref name="jdbc/mydbresource" binding-name="jdbc/mydbresource">  
  <authentication-alias name="auth1"/>  
</resource-ref>
```

---

## Configuring JAAS for database authentication

8.5.5.9

You can use Java Authentication and Authorization Service (JAAS) for database authentication.

### About this task

You can use a JAAS login context entry to specify a custom login module to use for setting the user name and password to authenticate to a database.

## Procedure

1. Add the `appSecurity-2.0`, `jdbc-4.0`, and `jca-1.6` features in the `server.xml` file. You can also add `appSecurity-2.0`, `jdbc-4.1`, and `jca-1.7`. For example:

```

<featureManager>
  <feature>appSecurity-2.0</feature>
  <feature>jdbc-4.0</feature>
  <feature>jca-1.6</feature>
</featureManager>

```

2. Configure a `jaasLoginContextEntry` element in the `server.xml` file with the login module to use. For example:

```

<jaasLoginContextEntry id="myJAASLoginEntry" name="myJAASLoginEntry" loginModuleRef="myLoginModule" />
<jaasLoginModule id="myLoginModule" className="my.package.MyLoginModule" controlFlag="REQUIRED" libraryRef="customLogin" />

<library id="customLoginLib">
  <fileset dir="${server.config.dir}" includes="MyLoginModule.jar"/>
</library>

```

3. Configure the `dataSource` element's `jaasLoginContextEntry` attribute with the id of the `jaasLoginContextEntry` element configured in step 2. For example:

```

<dataSource id="ds1" jndiName="jdbc/ds1" jdbcDriverRef="DB2"
  jaasLoginContextEntry="myJAASLoginEntry" .../>

```

4. As an alternative to step 3, you can configure a `custom-login-configuration` element in the deployment descriptor `ibm-web-bnd.xml` file of your application. The name attribute must match the id attribute for `jaasLoginContextEntry` that is defined in the `server.xml` file. For example:

```

<resource-ref name="jdbc/ds1ref" binding-name="jdbc/ds1">
  <custom-login-configuration name="myJAASLoginEntry">
    <property name="property1" value="value1"/>
  </custom-login-configuration>
</resource-ref>

```

---

## Developing extensions to the Liberty security infrastructure

The Liberty server provides various plug-in points so that you can extend the security infrastructure.

### About this task

The following topics are covered in this section:

#### Procedure

- Follow the instructions in “Developing a custom TAI for Liberty” to develop custom trust association interceptors (TAI) to extend the security infrastructure of Liberty server.
- Follow the instructions in “Developing JAAS custom login modules for a system login configuration” on page 2002 to develop JAAS custom login modules to extend the security infrastructure of Liberty server.

## Developing a custom TAI for Liberty

You can develop a custom trust association interceptor (TAI) class by implementing the `com.ibm.wsspi.security.tai.TrustAssociationInterceptor` interface provided in the Liberty server.

### About this task

The trust association interface is a service provider API that enables the integration of third-party security services with a Liberty server. When processing the web request, the Liberty server calls out and passes the `HttpServletRequest` and `HttpServletResponse` to the trust association interceptors. The `HttpServletRequest` calls the `isTargetInterceptor` method of the interceptor to see whether the interceptor can process the request. After an appropriate trust association interceptor is selected, the `HttpServletRequest` is processed by the `negotiateValidateandEstablishTrust` method of the interceptor, and the result is returned in a `TAIResult` object. You can add your own logic code to each method of the custom TAI class.

See also the Java API document for the TAI interface. The Java API documentation for each Liberty API is available in a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

**Avoid trouble:** **Distributed operating systems** **8.5.5.0** There are several security configuration examples on the WASdev.net website for reference when configuring security for your applications on Liberty. See “Configuring TAI on Liberty by using developer tools” on page 1891.

## Example

Here is a sample TAI class called SimpleTAI, which also lists all available methods from the TrustAssociationInterceptor interface.

```
package com.ibm.websphere.security.sample;

import java.util.Properties;

import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import com.ibm.websphere.security.WebTrustAssociationException;
import com.ibm.websphere.security.WebTrustAssociationFailedException;
import com.ibm.wsspi.security.tai.TAIResult;
import com.ibm.wsspi.security.tai.TrustAssociationInterceptor;

public class SimpleTAI implements TrustAssociationInterceptor {
    public SimpleTAI() {
        super();
    }

    /**
     * @see com.ibm.wsspi.security.tai.TrustAssociationInterceptor#isTargetInterceptor
     * (javax.servlet.http.HttpServletRequest)
     */
    public boolean isTargetInterceptor(HttpServletRequest req)
        throws WebTrustAssociationException {
        //Add logic to determine whether to intercept this request
        return true;
    }

    /**
     * @see com.ibm.wsspi.security.tai.TrustAssociationInterceptor#negotiateValidateandEstablishTrust
     * (javax.servlet.http.HttpServletRequest, javax.servlet.http.HttpServletResponse)
     */
    public TAIResult negotiateValidateandEstablishTrust(HttpServletRequest req,
        HttpServletResponse resp) throws WebTrustAssociationFailedException {
        // Add logic to authenticate a request and return a TAI result.
        String tai_user = "taiUser";
        return TAIResult.create(HttpServletResponse.SC_OK, tai_user);
    }

    /**
     * @see com.ibm.wsspi.security.tai.TrustAssociationInterceptor#initialize(java.util.Properties)
     */
    public int initialize(Properties arg0)
        throws WebTrustAssociationFailedException {
        return 0;
    }

    /**
     * @see com.ibm.wsspi.security.tai.TrustAssociationInterceptor#getVersion()
     */
}
```

```

    public String getVersion() {
        return "1.0";
    }

    /*
    * @see com.ibm.wsspi.security.tai.TrustAssociationInterceptor#getType()
    */
    public String getType() {
        return this.getClass().getName();
    }

    /*
    * @see com.ibm.wsspi.security.tai.TrustAssociationInterceptor#cleanup()
    */
    public void cleanup()

    {}
}

```

## What to do next

Add the TAI class to the Liberty server.

Use one of the following methods to add the TAI class to the Liberty server:

- Put the custom TAI class in a JAR file, for example `simpleTAI.jar`, then make the JAR file available as a shared library. See “Configuring TAI in Liberty” on page 1889.
- Package the custom TAI class as a feature. See “Developing a custom TAI as a Liberty feature” on page 1820.

## Developing a custom SIP TAI

8.5.5.7

When you develop Session Initiation Protocol (SIP) applications, you can create a custom trust association interceptor (TAI).

### Before you begin

Developing a SIP TAI is similar to developing any other custom interceptors used in trust associations. In fact, a custom TAI for a SIP application is an extension of the trust association interceptor model.

### About this task

TAI can be invoked by a SIP servlet request or a SIP servlet response. To implement a custom SIP TAI, you need to write your own Java class.

### Procedure

1. Write a Java class that extends the `com.ibm.wsspi.security.tai.extension.BaseTrustAssociationInterceptor` class and implements the `com.ibm.websphere.security.tai.extension.SIPTrustAssociationInterceptor` interface. Those classes are defined in the `${wlp.install.dir}/dev/api/ibm/ccom.ibm.websphere.appserver.api.sipServletSecurity.1.0_1.0.10.jar` file.
2. Declare the following Java methods:

```
public int initialize(Properties properties) throws WebTrustAssociationFailedException;
```

This is invoked before the first message is processed so that the implementation can allocate any resources that it needs. For example, it might establish a connection to a database.

WebTrustAssociationFailedException is defined in the `{wlp.install.dir}/lib/com.ibm.websphere.security_1.0.10.jar` file. The value of the properties argument comes from the `<trustAssociation>` configuration.

**public void cleanup();**

This is invoked when the TAI can free any resources that it holds. For example, it could close a connection to a database.

**public boolean isTargetProtocolInterceptor(SipServletMessage sipMsg) throws WebTrustAssociationFailedException;**

Your custom TAI can use this method to handle the sipMsg message. If the method returns false, WebSphere ignores your TAI for sipMsg.

**public TAIResult negotiateValidateandEstablishProtocolTrust (SipServletRequest req, SipServletResponse resp) throws WebTrustAssociationFailedException;**

This method returns a TAIResult that indicates the status of the message that is being processed and a user ID or the unique ID for the user who is trying to authenticate. If authentication succeeds, the TAIResult contains the status `HttpServletResponse.SC_OK` and a principal. If authentication fails, the TAIResult will contain a return code of `HttpServletResponse.SC_UNAUTHORIZED (401)`, `SC_FORBIDDEN (403)`, or `SC_PROXY_AUTHENTICATION_REQUIRED (407)`. This only indicates whether the container should accept a message for further processing. To challenge an incoming request, the TAI implementation must generate and send its own `SipServletResponse` containing a challenge. The exception can be thrown for internal TAI errors. Table 1 describes the argument values and resultant actions for the `negotiateValidateandEstablishProtocolTrust` method.

Table 135. Description of negotiateValidateandEstablishProtocolTrust arguments and actions.

This table provides a description of the `negotiateValidateandEstablishProtocolTrust` arguments and actions

Argument or action	For a SIP request	For a SIP response
Value of req argument	The incoming request	Null
Value of resp argument	Null	The incoming response
Action for valid response credentials	Return <code>TAIResult.status</code> containing <code>SC_OK</code> and a user ID or unique ID	Return <code>TAIResult.status</code> containing <code>SC_OK</code> and a user ID or unique ID
Action for incorrect response credentials	Return the <code>TAIResult</code> with the 4xx status	Return the <code>TAIResult</code> with the 4xx status

The sequence of events is as follows:

- a. The SIP container maps initial requests to applications by using the rules in each applications deployment descriptor; subsequent messages are mapped based on JSR289 mechanisms.
- b. If any of the applications require security, the SIP container invokes any defined TAI implementations for the message.
- c. If the message passes security, the container invokes the corresponding applications.

Your TAI implementation can modify a SIP message, but the modified message will not be usable within the request mapping process, because it finishes before the container invokes the TAI.

The `com.ibm.wsspi.security.tai.TAIResult` class, which is defined in the `{wlp.install.dir}/lib/com.ibm.ws.security.authentication.tai_1.0.10.jar` file, has three static methods for creating a `TAIResult`. The `TAIResult` create methods take an `int` type as the first parameter. The WebSphere Application Server expects the result to be a valid HTTP request return code and is interpreted as follows:

If the value is `HttpServletResponse.SC_OK`, this response tells WebSphere that the TAI has completed its negotiation. The response also tells WebSphere to use the information in the `TAIResult` to create a user identity.

The created `TAIResults` have the meanings that are shown in Table 2.

Table 136. Meanings of `TAIResults`.

This table lists the meanings of `TAIResults`

TAIResult	Explanation
<code>public static TAIResult create(int status);</code>	Indicates a status to the WebSphere Application Server. The status should not be <code>SC_OK</code> because the identity information is provided.
<code>public static TAIResult create(int status, String principal);</code>	Indicates a status to the WebSphere Application Server and provides the user ID or the unique ID for this user. WebSphere creates credentials by querying the user registry.
<code>public static TAIResult create(int status, String principal, Subject subject);</code>	Indicates a status to the WebSphere Application Server, the user ID or the unique ID for the user, and a custom Subject. If the Subject contains a Hashtable, the principal is ignored. The contents of the Subject becomes part of the eventual user Subject.

**public String getVersion();**

This method returns the version number of the current TAI implementation.

**public String getType();**

This method's return value is implementation-dependent.

3. Compile the implementation after you have implemented it to create your own SIP TAI jar file.
4. Follow steps 3-4 described in the topic [Configuring TAI for Liberty](#) to configure the Liberty server to use the SIP TAI.

## Developing JAAS custom login modules for a system login configuration

For a Liberty server, multiple Java Authentication and Authorization Service (JAAS) plug-in points exist for configuring system logins. The Liberty uses system login configurations to authenticate incoming requests. You can develop a custom JAAS login module to add information to the **Subject** of a system login configuration.

### About this task

Application login configurations are called by servlet applications for obtaining a Subject that is based on specific authentication information. When you write a login module that plugs into a Liberty profile application login or system login configuration, you must develop login configuration logic that knows when specific information is present, and how to use the information. See ["JAAS configuration"](#) on page 978 and ["JAAS login modules"](#) on page 979 for more details.

To develop a JAAS custom login module for a system login configuration, follow the steps in the procedure:

### Procedure

- Understand usable callbacks and how they work.

See [Programmatic login for JAAS](#) for more information about usable callbacks.

**Note:** Liberty only supports the following callbacks:

```
callbacks[0] = new javax.security.auth.callback.NameCallback("Username: ");
callbacks[1] = new javax.security.auth.callback.PasswordCallback("Password: ", false);
callbacks[2] = new com.ibm.websphere.security.auth.callback.WSCredTokenCallbackImpl("Credential Token: ");
```

```

callbacks[3] = new com.ibm.websphere.security.auth.callback.WSServletRequestCallback("HttpServletRequest: ");
callbacks[4] = new com.ibm.websphere.security.auth.callback.WSServletResponseCallback("HttpServletResponse: ");
callbacks[5] = new com.ibm.websphere.security.auth.callback.WSAppContextCallback("ApplicationContextCallback: ");
callbacks[6] = new WSRealmNameCallbackImpl("Realm Name: ", default_realm);
callbacks[7] = new WSX509CertificateChainCallback("X509Certificate[]: ");
callbacks[8] = wsAuthMechOidCallback = new WSAuthMechOidCallbackImpl("AuthMechOid: ");

```

- Understand shared state variables and how they work.

If you want to access the objects that the WebSphere Application Server traditional creates during a login, refer to the following shared state variables. For more information about these variables, see the “System Programming Interfaces” subtopic of Programming Interfaces

#### **com.ibm.wsspi.security.auth.callback.Constants.WSPRINCIPAL\_KEY**

Specifies an implemented object of the java.security.Principal interface. This shared state variable is for read-only purposes. Do not set this variable in the shared state for custom login modules. The default login module sets this variable.

#### **com.ibm.wsspi.security.auth.callback.Constants.WSCREDENTIAL\_KEY**

Specifies the com.ibm.websphere.security.cred.WSCredential object. This shared state variable is for read-only purposes. Do not set this variable in the shared state for custom login modules. The default login module will set this variable.

#### **com.ibm.wsspi.security.auth.callback.Constants.WSSSOTOKEN\_KEY**

Specifies the com.ibm.wsspi.security.token.SingleSignonToken object. Do not set this variable in the shared state for custom login modules. The default login module sets this variable.

- Optional: Understand hashtables for custom JAAS login modules in Liberty. See “Hash table login module” on page 985 for more details.
- Develop a sample custom login module using callbacks and shared state.

You can use the following sample to learn on how to use some of the callbacks and shared state variables.

```

public class CustomCallbackLoginModule implements LoginModule {

    protected Map<String, ?> _sharedState;
    protected Subject _subject = null;
    protected CallbackHandler _callbackHandler;
    private final String customPrivateCredential = "CustomLoginModuleCredential";

    /**
     * Initialization of login module
     */
    public void initialize(Subject subject, CallbackHandler callbackHandler,
        Map<String, ?> sharedState, Map<String, ?> options) {
        _sharedState = sharedState;
        _subject = subject;
        _callbackHandler = callbackHandler;
    }

    public boolean login() throws LoginException {
        try {
            AccessController.doPrivileged(new PrivilegedExceptionAction<Object>() {
                public Object run() throws Exception {
                    _subject.getPrivateCredentials().add(customPrivateCredential);
                    return null;
                }
            });
        } catch (PrivilegedActionException e) {
            throw new LoginException(e.getLocalizedMessage());
        }

        String username = null;
        char passwordChar[] = null;
        byte[] credToken = null;
        HttpServletRequest request = null;
        HttpServletResponse response = null;
        Map appContext = null;
        String realm = null;
        String authMechOid = null;
        java.security.cert.X509Certificate[] certChain = null;

```

```

NameCallback nameCallback = null;
PasswordCallback passwordCallback = null;
WSCredTokenCallbackImpl wsCredTokenCallback = null;
WSServletRequestCallback wsServletRequestCallback = null;
WSServletResponseCallback wsServletResponseCallback = null;
WSAppContextCallback wsAppContextCallback = null;
WSRealmNameCallbackImpl wsRealmNameCallback = null;
WSX509CertificateChainCallback wsX509CertificateCallback = null;
WSAuthMechOidCallbackImpl wsAuthMechOidCallback = null;

Callback[] callbacks = new Callback[9];
callbacks[0] = nameCallback = new NameCallback("Username: ");
callbacks[1] = passwordCallback = new PasswordCallback("Password: ", false);
callbacks[2] = wsCredTokenCallback = new WSCredTokenCallbackImpl("Credential Token: ");
callbacks[3] = wsServletRequestCallback = new WSServletRequestCallback("HttpServletRequest: ");
callbacks[4] = wsServletResponseCallback = new WSServletResponseCallback("HttpServletResponse: ");
callbacks[5] = wsAppContextCallback = new WSAppContextCallback("ApplicationContextCallback: ");
callbacks[6] = wsRealmNameCallback = new WSRealmNameCallbackImpl("Realm name:");
callbacks[7] = wsX509CertificateCallback = new WSX509CertificateChainCallback("X509Certificate[]: ");
callbacks[8] = wsAuthMechOidCallback = new WSAuthMechOidCallbackImpl("AuthMechOid: ");

try {
    _callbackHandler.handle(callbacks);
} catch (Exception e) {
    // handle exception
}

if (nameCallback != null)
    username = nameCallback.getName();

if (passwordCallback != null)
    passwordChar = passwordCallback.getPassword();

if (wsCredTokenCallback != null)
    credToken = wsCredTokenCallback.getCredToken();

if (wsServletRequestCallback != null)
    request = wsServletRequestCallback.getHttpServletRequest();

if (wsServletResponseCallback != null)
    response = wsServletResponseCallback.getHttpServletResponse();

if (wsAppContextCallback != null)
    appContext = wsAppContextCallback.getContext();

if (wsRealmNameCallback != null)
    realm = wsRealmNameCallback.getRealmName();

if (wsX509CertificateCallback != null)
    certChain = wsX509CertificateCallback.getX509CertificateChain();

if (wsAuthMechOidCallback != null)
    authMechOid = wsAuthMechOidCallback.getAuthMechOid();

_subject.getPrivateCredentials().add("username = " + username);
_subject.getPrivateCredentials().add("password = " + String.valueOf(passwordChar));
_subject.getPrivateCredentials().add("realm = " + realm);
_subject.getPrivateCredentials().add("authMechOid = " + authMechOid.toString());

return true;
}

public boolean commit() throws LoginException {
    return true;
}

public boolean abort() {
    return true;
}

public boolean logout() {
    return true;
}
}

```

- Optional: Develop a sample custom login module using hashtable login. You can use the following sample to learn on how to use hashtable login.

```

package com.ibm.websphere.security.sample;

import java.util.Map;

import javax.security.auth.Subject;
import javax.security.auth.callback.CallbackHandler;
import javax.security.auth.login.LoginException;
import javax.security.auth.spi.LoginModule;

import com.ibm.wsspi.security.token.AttributeNameConstants;

/**
 * Custom login module that adds another PublicCredential to the subject
 */
@SuppressWarnings("unchecked")
public class CustomHashtableLoginModule implements LoginModule {

    protected Map<String, ?> _sharedState;
    protected Map<String, ?> _options;

    /**
     * Initialization of login module
     */
    public void initialize(
        Subject subject, CallbackHandler callbackHandler, Map<String, ?> sharedState, Map<String, ?> options) {
        _sharedState = sharedState;
        _options = options;
    }

    public boolean login() throws LoginException {
        try {
            java.util.Hashtable<String, Object> customProperties = (java.util.Hashtable<String, Object>)
                _sharedState.get(AttributeNameConstants.WSCREDENTIAL_PROPERTIES_KEY);
            if (customProperties == null) {
                customProperties = new java.util.Hashtable<String, Object>();
            }

            customProperties.put(AttributeNameConstants.WSCREDENTIAL_USERID, "userId");
            // Sample of creating custom cache key
            customProperties.put(AttributeNameConstants.WSCREDENTIAL_CACHE_KEY, "customCacheKey");

            /*
             * Sample for creating user ID and security name
             * customProperties.put(AttributeNameConstants.WSCREDENTIAL_UNIQUEID, "userId");
             * customProperties.put(AttributeNameConstants.WSCREDENTIAL_SECURITYNAME, "securityName");
             * customProperties.put(AttributeNameConstants.WSCREDENTIAL_REALM, "realm");
             * customProperties.put(AttributeNameConstants.WSCREDENTIAL_GROUPS, "groupList");
             */
            /*
             * Sample for creating user ID and password
             * customProperties.put(AttributeNameConstants.WSCREDENTIAL_USERID, "userId");
             * customProperties.put(AttributeNameConstants.WSCREDENTIAL_PASSWORD, "password");
             */
            Map<String, java.util.Hashtable> mySharedState = (Map<String, java.util.Hashtable>) _sharedState;
            mySharedState.put(AttributeNameConstants.WSCREDENTIAL_PROPERTIES_KEY, customProperties);
        } catch (Exception e) {
            throw new LoginException("LoginException: " + e.getMessage());
        }

        return true;
    }

    public boolean commit() throws LoginException {
        return true;
    }

    public boolean abort() {
        return true;
    }

    public boolean logout() {
        return true;
    }
}

```

## What to do next

Add your custom login module into the WEB\_INBOUND, and DEFAULT Java Authentication and Authorization Service (JAAS) system login configurations of the server.xml file. Put the custom login module class in a JAR file, for example, customLoginModule.jar, then make the JAR file available to the Liberty server. See “Configuring a JAAS custom login module for Liberty” on page 1868.

## Developing a custom JASPIC authentication provider for Liberty



8.5.5.6

You can develop a custom Java Authentication SPI for Containers (JASPIC) authentication provider by creating classes that implement the required interfaces noted in the JSR 196: Java Authentication Service Provider Interface for Containers specification.

### Before you begin

Review the specific interface implementation requirements for JASPIC authentication providers and modules in the JSR 196: Java Authentication Service Provider Interface for Containers specification.

### About this task

WebSphere Application Server Liberty supports the use of third-party authentication providers that are compliant with the servlet container profile specified in Java Authentication SPI for Containers (JASPIC) Version 1.1.

The servlet container profile defines interfaces that are used by the security runtime environment in collaboration with the web container in the WebSphere Application Server to invoke authentication modules before and after a web request is processed by an application. Authentication that uses JASPIC modules is performed only when JASPIC is enabled in the security configuration.

To develop a custom authentication provider, create classes that implement the required interfaces noted in the JSR 196: Java Authentication Service Provider Interface for Containers specification. A provider can use one or more authentication modules for authentication. Modules can use callbacks to perform authentication, or they can manually add the necessary user identity information to the client subject.

### Procedure

1. Create a class that implements the `javax.security.auth.message.config.AuthConfigProvider` interface.

The `AuthConfigProvider` implementation class must define a public two-argument constructor and the `getServerAuthConfig` public method:

```
import java.util.Map;
import javax.security.auth.callback.CallbackHandler;
import javax.security.auth.message.AuthException;
import javax.security.auth.message.config.AuthConfigFactory;
import javax.security.auth.message.config.AuthConfigProvider;
import javax.security.auth.message.config.ServerAuthConfig;

public class SampleAuthConfigProvider implements AuthConfigProvider {

    public SampleAuthConfigProvider(Map<String, String> properties, AuthConfigFactory factory) {
        ...
    }
    public ServerAuthConfig getServerAuthConfig(String layer, String appContext, CallbackHandler handler)
        throws AuthException {
        ...
    }
}
```

An instance of the `AuthConfigProvider` implementation class is used by WebSphere Application Server when a request arrives to be processed by the web module of the application. The `getServerAuthConfig` method is used to obtain a `ServerAuthConfig` instance. The `CallbackHandler` argument in the method call is used by the authentication module.

2. Create a class that implements the `javax.security.auth.message.config.ServerAuthConfig` interface. The `ServerAuthConfig` implementation class must define the `getAuthContextID` and `getAuthContext` public methods:

```
import java.util.Map;
import javax.security.auth.Subject;
import javax.security.auth.message.AuthException;
import javax.security.auth.message.MessageInfo;
import javax.security.auth.message.config.ServerAuthConfig;
import javax.security.auth.message.config.ServerAuthContext;

public class SampleServerAuthConfig implements ServerAuthConfig {

    public String getAuthContextID(MessageInfo messageInfo) throws IllegalArgumentException {
        ...
    }
    public ServerAuthContext getAuthContext(String authContextID, Subject serviceSubject, Map properties)
        throws AuthException {
        ...
    }
}
```

The `getAuthContextID` and `getAuthContext` methods in the `ServerAuthConfig` implementation class are used to obtain a `ServerAuthContext` instance.

3. Create a class that implements the `javax.security.auth.message.config.ServerAuthContext` interface. The `ServerAuthContext` implementation class must define the `validateRequest` and `secureResponse` public methods:

```
import javax.security.auth.Subject;
import javax.security.auth.message.AuthException;
import javax.security.auth.message.AuthStatus;
import javax.security.auth.message.MessageInfo;
import javax.security.auth.message.config.ServerAuthContext;

public class SampleServerAuthContext implements ServerAuthContext {

    public AuthStatus validateRequest(MessageInfo messageInfo, Subject clientSubject, Subject serviceSubject)
        throws AuthException {
        ...
    }
    public AuthStatus secureResponse(MessageInfo messageInfo, Subject serviceSubject)
        throws AuthException {
        ...
    }
}
```

The `validateRequest` method in the `ServerAuthContext` implementation class is used to invoke the module that authenticates the received web request message. If the authentication result is successful, the web container dispatches the received web request message that the target web module processes in the application. If the authentication result is not successful, the request is rejected with the appropriate response status.

4. Create a class that implements the `javax.security.auth.message.module.ServerAuthModule` interface. The `ServerAuthModule` implementation class must define the `initialize`, `validateRequest`, and `secureResponse` public methods:

```
import javax.security.auth.Subject;
import javax.security.auth.callback.CallbackHandler;
import javax.security.auth.message.AuthException;
import javax.security.auth.message.AuthStatus;
import javax.security.auth.message.MessageInfo;
import javax.security.auth.message.MessagePolicy;
```

```

import javax.security.auth.message.module.ServerAuthModule;

public class SampleAuthModule implements ServerAuthModule {

    public void initialize(MessagePolicy requestPolicy, MessagePolicy responsePolicy, CallbackHandler handler, Map<String, Object> context) throws AuthException {
        ...
    }

    public AuthStatus validateRequest(MessageInfo messageInfo, Subject clientSubject, Subject serviceSubject) throws AuthException {
        ...
    }

    public AuthStatus secureResponse(MessageInfo messageInfo, Subject serviceSubject) throws AuthException {
        ...
    }

    public void cleanSubject(MessageInfo messageInfo, Subject subject) throws AuthException {
        ...
    }
}

```

The `initialize` method in the `ServerAuthModule` implementation class is called by the `ServerAuthContext` implementation class to initialize the authentication module and to associate it with the `ServerAuthContext` instance.

The `validateRequest` and `secureResponse` methods in this class are used to authenticate the `javax.servlet.http.HttpServletRequest` and `javax.servlet.http.HttpServletResponse` contained in the `javax.security.auth.message.MessageInfo` that is received. These methods can use the `CallbackHandler` instance that is received in the `initialize` method to interact with the WebSphere security run time to validate a user password, and the active user registry to retrieve a unique id and group membership for a user. The retrieved data is placed in a `Hashtable` in the set of private credentials in the client subject. The WebSphere Application Server implementation of the `CallbackHandler` supports the following three callbacks:

- `CallerPrincipalCallback`
- `GroupPrincipalCallback`
- `PasswordValidationCallback`

WebSphere Application Server expects the name values obtained with `PasswordValidationCallback.getUsername()` and `CallerPrincipalCallback.getName()` to be identical. If they are not, unpredictable results occur. The `handle()` method of the `CallbackHandler` processes each callback that is given in the argument array of the method sequentially. Therefore, the name value set in the private credentials of the client subject is the one obtained from the last callback processed.

If `CallbackHandler` is not used by the authentication module, and `validateRequest` returns a successful status, WebSphere Application Server requires that a `Hashtable` instance be included in the `clientSubject` with user identity information so that a custom login can be performed to obtain the credentials for the user. This `Hashtable` can be added to the client subject as in the following example:

```

import java.util.Hashtable;
import java.util.String;
import javax.security.auth.Subject;
import javax.security.auth.message.AuthException;
import javax.security.auth.message.AuthStatus;
import javax.security.auth.message.MessageInfo;
import com.ibm.wsspi.security.registry.RegistryHelper;
import com.ibm.wsspi.security.token.AttributeNameConstants.AttributeNameConstants;

public AuthStatus validateRequest(MessageInfo messageInfo, Subject clientSubject, Subject serviceSubject) throws AuthException {
    ...
}

```

```

UserRegistry reg = RegistryHelper.getUserRegistry(null);
String uniqueid = reg.getUniqueUserID(username);

Hashtable hashtable = new Hashtable();
hashtable.put(AttributeConstants.WSCREDENTIAL_UNIQUEID, uniqueid);
hashtable.put(AttributeConstants.WSCREDENTIAL_SECURITYNAME, username);
hashtable.put(AttributeConstants.WSCREDENTIAL_PASSWORD, password);
hashtable.put(AttributeConstants.WSCREDENTIAL_GROUPS, groupList); //optional
clientSubject.getPrivateCredentials().add(hashtable);
...
}

```

For more information about the Hashtable requirements and custom login, see Developing JAAS custom login modules for a system login configuration.

## Developing a Java Authorization Contract for Containers (JACC) Authorization Provider



8.5.5.6

You can develop a JACC provider to have custom authorization decisions for Java Platform, Enterprise Edition (J2EE) applications by implementing the `com.ibm.wsspi.security.authorization.jacc.ProviderService` interface that is provided in the Liberty server.

### Before you begin

By default, the application module loading is deferred until the request to the application is being processed, however the security constraint of the entire module in the application needs to be processed before the application is ready to be processed. The deferred module loading needs to be disabled. The following shows you how to disable it:

1. For the WebContainer:

In the `server.xml` file, the following element needs to be set:

```
<webContainer deferServletLoad="false"/>
```

2. For the EJBContainer:

In the `server.xml` file, the following element needs to be set:

```
<ejbContainer startEJBsAtAppStart="true"/>
```

**Note:** If the previous elements are not set, the complete security constraint information may not be propagated to the third party JACC provider upon starting the server. As a result, the correct authorization decision may not be enforced by the third party JACC provider.

### About this task

The Java Authorization Contract for Containers specification, JSR 115, defines an interface for authorization providers. In the Liberty server, you must package your JACC provider as a user feature. Your feature must implement the `com.ibm.wsspi.security.authorization.jacc.ProviderService` interface.

### Procedure

1. Create an OSGi component that provides a service that implements the `com.ibm.wsspi.security.authorization.jacc.ProviderService` interface.

The `ProviderService` interface defines two methods, `getPolicy`, which the Liberty server run time invokes to retrieve an instance of your `Policy` class that implements the `java.security.Policy` abstract class, and `getPolicyConfigFactory`, which the Liberty server run time invokes to retrieve an instance

of your PolicyConfigurationFactory class that implements the javax.security.jacc.PolicyConfigurationFactory abstract class. The following example uses OSGi declarative services annotations:

```

package com.mycompany.jacc;

import com.mycompany.jacc.MyAuthConfigProvider;
import com.ibm.wsspi.security.authorization.jacc.ProviderService;
import java.security.Policy;
import java.util.Map;
import javax.security.jacc.PolicyConfigurationFactory;
import org.osgi.service.component.ComponentContext;
import org.osgi.service.component.annotations.Activate;
import org.osgi.service.component.annotations.Component;
import org.osgi.service.component.annotations.Deactivate;

// The property value of javax.security.jacc.policy.provider which defines the implementation class of Policy and
// javax.security.jacc.PolicyConfigurationFactory.provider which defines the implementation class of PolicyConfiguration
@Component(service = ProviderService.class,
    immediate = true,
    property = {
        "javax.security.jacc.policy.provider=com.myco.jacc.MyPolicy",
        "javax.security.jacc.PolicyConfigurationFactory.provider="
        + "com.myco.jacc.MyFactoryImpl"
    }
)

public class MyJaccProviderService implements ProviderService {
    Map<String, String> configProps;

    // This method called by the Liberty runtime
    // to get an instance of Policy class
    @Override
    public Policy getPolicy() {
        return new myPolicy();
    }

    // This method called by the Liberty runtime
    // to get an instance of PolicyConfigurationFactory class
    @Override
    public PolicyConfigurationFactory getPolicyConfigurationFactory() {
        ClassLoader cl = null;
        PolicyConfigurationFactory pcf = null;
        System.setProperty(
            "javax.security.jacc.PolicyConfigurationFactory.provider",
            "com.myco.jacc.MyFactoryImpl");
        try {
            cl = Thread.currentThread().getContextClassLoader();
            Thread.currentThread().setContextClassLoader(
                this.getClass().getClassLoader());
            pcf = PolicyConfigurationFactory.getPolicyConfigurationFactory();
        } catch (Exception e) {
            return null;
        } finally {
            Thread.currentThread().setContextClassLoader(cl);
        }
        return pcf;
    }

    @Activate
    protected void activate(ComponentContext cc) {
        // Read provider config properties here if needed,
        // then pass them to the Provider ctor.
        // This example reads the properties from the OSGi
        // component definition.
        configProps = (Map<String, String>) cc.getProperties();
    }
}

```

```

    }

    @Deactivate
    protected void deactivate(ComponentContext cc) {}
}

```

2. Package the component into an OSGi bundle that is part of your user feature, along with your JACC provider.
3. Ensure that your feature includes the OSGi subsystem content: `com.ibm.ws.javaee.jacc.1.5; version="[1,1.0.100)"; location="dev/api/spec/"`.
4. After the feature is installed into the user product extension location, configure the `server.xml` file with the feature name. For example:

```

<featureManager>
    ...
    <feature>usr:myJaccProvider</feature>
</featureManager>

```

## Developing a customPasswordEncryption Provider

8.5.5.9

You can develop a `customPasswordEncryption` provider to have custom authorization decisions for Java Platform, Enterprise Edition (J2EE) applications by implementing the `com.ibm.wsspi.security.crypto.CustomPasswordEncryption` interface that is provided in the Liberty server.

### About this task

#### Procedure

1. Create an OSGi component that provides a service that implements the `com.ibm.wsspi.security.crypto.CustomPasswordEncryption` interface.

The `CustomPasswordEncryption` interface defines three methods, `decrypt`, which the Liberty server run time invokes to decrypt the string, `encrypt`, which the Liberty server run time invokes to encrypt the string, and `initialize`, which is reserved for future use.

The following example uses OSGi declarative services annotations:

```

package com.mycompany.custom;

import org.osgi.service.component.ComponentContext;
import org.osgi.service.component.annotations.Activate;
import org.osgi.service.component.annotations.Component;
import org.osgi.service.component.annotations.ConfigurationPolicy;
import org.osgi.service.component.annotations.Deactivate;
import org.osgi.service.component.annotations.Modified;

import com.ibm.wsspi.security.crypto.CustomPasswordEncryption;
import com.ibm.wsspi.security.crypto.EncryptedInfo;
import com.ibm.wsspi.security.crypto.PasswordDecryptException;
import com.ibm.wsspi.security.crypto.PasswordEncryptException;

/**
 */
@Component(service = CustomPasswordEncryption.class,
           immediate = true,
           name = "com.mycompany.CustomPasswordEncryptionImpl",
           configurationPolicy = ConfigurationPolicy.OPTIONAL,
           property = { "someKey=someValue" })
public class CustomPasswordEncryptionImpl implements CustomPasswordEncryption {

    @Activate
    protected synchronized void activate(ComponentContext cc, Map<String, Object> props) {
    }
}

```

```

@Modified
protected synchronized void modify(Map<String, Object> props) {
}

@Deactivate
protected void deactivate(ComponentContext cc) {
}

/**
 * The encrypt operation takes a UTF-8 encoded String in the form of a byte[].
 * The byte[] is generated from String.getBytes("UTF-8"). An encrypted byte[]
 * is returned from the implementation in the EncryptedInfo object.
 * Additionally, a logically key alias is returned in EncryptedInfo so which
 * is passed back into the decrypt method to determine which key was used to
 * encrypt this password. The WebSphere Application Server runtime has no
 * knowledge of the algorithm or key used to encrypt the data.
 *
 * @param decrypted_bytes
 * @return com.ibm.wsspi.security.crypto.EncryptedInfo
 * @throws com.ibm.wsspi.security.crypto.PasswordEncryptException
 */
@Override
public EncryptedInfo encrypt(byte[] input) throws PasswordEncryptException {
    byte[] output = null;
    String key = null;
    try {
        :
        <do some encryption>
        :
        return new EncryptedInfo(output, key);
    } catch (Exception e) {
        throw new PasswordEncryptException("Exception is caught", e);
    }
}

/**
 * The decrypt operation takes the EncryptedInfo object containing a byte[]
 * and the logical key alias and converts it to the decrypted byte[]. The
 * WebSphere Application Server runtime will convert the byte[] to a String
 * using new String (byte[], "UTF-8");
 *
 * @param info
 * @return byte[]
 * @throws PasswordEncryptException
 * @throws com.ibm.wsspi.security.crypto.PasswordDecryptException
 */
@Override
public byte[] decrypt(EncryptedInfo info) throws PasswordDecryptException {
    byte[] input = info.getEncryptedBytes();
    String key = info.getKeyAlias();
    byte[] output = null;
    try {
        :
        <do some decryption>
        :
        return output;
    } catch (Exception e) {
        throw new PasswordEncryptException("Exception is caught", e);
    }
}

/**
 * This is reserved for future use and is currently not called by the
 * WebSphere Application Server runtime.
 *
 * @param initialization_data

```

```

    **/
    @SuppressWarnings("rawtypes")
    @Override
    public void initialize(Map initialization_data) {}
}

```

2. Package the component into an OSGi bundle that is part of your user feature. Make sure that the bundle includes the OSGi service manifest.

The following example shows the contents of OSGi service manifest:

```

<?xml version="1.0" encoding="UTF-8"?>
<scr:component xmlns:scr="http://www.osgi.org/xmlns/scr/v1.1.0" name="com.mycompany.custom.CustomPasswordEncryptionImpl">
  <implementation class="com.mycompany.custom.CusomPasswordEncryptionImpl"/>
  <service>
    <provide interface="com.ibm.wsspi.security.crypto.CustomPasswordEncryption"/>
  </service>
  <property name="<someKey>" type="String" value="<someValue>"/>
</scr:component>

```

3. Ensure that your feature manifest includes the OSGi subsystem content with start-phase:="SERVICE\_EARLY". For example:

```

Manifest-Version: 1.0
IBM-Feature-Version: 2
IBM-ShortName: customPasswordEncryption-1.0
Subsystem-Type: osgi.subsystem.feature
Subsystem-Version: 1.0.0
Subsystem-ManifestVersion: 1.0
Subsystem-SymbolicName: customPasswordEncryption-1.0;visibility:=public
Subsystem-Content:
com.mycompany.custom; version="[1,1.0.100)"; start-phase:="SERVICE_EARLY"

```

4. After the feature is installed into the user product extension location, configure the server.xml file with the feature name.

```

<featureManager>
  ...
  <feature>usr:customPasswordEncryption-1.0</feature>
</featureManager>

```

## Customizing an application login to perform an identity assertion by using JAAS

You can use the Java Authentication and Authorization Service (JAAS) login framework to create a JAAS login configuration that can be used to perform login to an identity assertion on Liberty.

### About this task

By configuring identity assertion with trust validation, an application can use the JAAS login configuration to perform a programmatic identity assertion. See `IdentityAssertionLoginModule` for more detail.

**Avoid trouble:** Distributed operating systems 8.5.5.0 There are several security configuration examples on the WASdev.net website for reference when configuring security for your applications on Liberty. See “Configuring JAAS on Liberty by using developer tools” on page 1870.

### Procedure

1. Delegate trust validation to a user-implemented plug-in point.

Trust validation is accomplished by a custom login module. This custom login module performs any trust validation required, then sets the trust and identity information in the shared state to be passed on to the identity assertion login module. A map is required in the following shared state key:

```
com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.state
```

If the state is missing then a `WSLoginFailedException` problem is reported by the `IdentityAssertionLoginModule` class.

The map in the shared state key must include a trust key with the following key name:

```
com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.trust
```

If this key is set to true, then trust is established. If the key is set to false, then no trust is established and `IdentityAssertionLoginModule` class creates a `WSLoginFailedException` problem.

The map in the shared state key must also set one of the following resources:

- An identity key. A `java.security.Principal` can be set in the following key:  
`com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.principal`
- A `java.security.cert.X509Certificate[]`. This certificate can be set in the following key:  
`com.ibm.wsspi.security.common.auth.module.IdentityAssertionLoginModule.certificates`

If both a principal and certificate are supplied, then the principal is used and a warning is reported.

2. Create a JAAS configuration for application logins. The JAAS configuration will contain the user-implemented trust validation custom login module and `IdentityAssertionLoginModule` class. Then to configure an application login configuration, add the following code in the `server.xml` file:

```
<jaasLoginContextEntry id="CustomIdentityAssertion" name="CustomIdentityAssertion"
    loginModuleRef="customIdentityAssertion,identityAssertion" />
<jaasLoginModule id="customIdentityAssertion"
    className="com.ibm.ws.security.authentication.IdentityAssertionLoginModule"
    controlFlag="REQUIRED" libraryRef="customLoginLib"/>
<library id="customLoginLib">
    <fileset dir="{server.config.dir}" includes="IdentityAssertionLoginModule.jar"/>
</library>
```

This JAAS configuration is used by the application to perform an identity assertion.

3. Perform the programmable identity assertion. A program can now use the JAAS login configuration to perform a programmatic identity assertion. The application program can create a login context for the JAAS configuration created in step 2, then log in to that login context with the identity that would assert to. If the login is successful then that identity can be set in the current running process. The following example illustrates this process:

```
NameCallback handler = new NameCallback(new MyPrincipal("Joe"));
LoginContext lc = new LoginContext("customIdentityAssertion", handler);
lc.login(); //assume successful
Subject s = lc.getSubject();
WSSubject.setRunAsSubject(s);
// From here on , the runas identity is "Joe"
```

**Note:** The `MyPrincipal` class is the implementation of the `java.security.Principal` interface in the example.

## Results

Using the JAAS login framework and two user-implemented login modules, you can create a JAAS login configuration that can be used to log in to an identity assertion.

## Developing a custom user registry in Liberty

8.5.5.0

You can develop a custom user registry class by implementing the `com.ibm.websphere.security.UserRegistry` interface provided in the Liberty server.

## About this task

The `UserRegistry` interface is a Service Programming Interface (SPI) that enables support to virtually any type of account repository. For a general view of stand-alone custom registries, see [Stand-alone custom registries](#).

### Procedure

1. Implement the custom user registry. For more information, see [Developing the UserRegistry interface for using custom registries](#).
2. Convert the implementation class into an OSGi service. You can do the conversion in the following ways:
  - Convert your `UserRegistry` class into a Declarative Service (DS) component. For more information, see [“Declaring your services to OSGi Declarative Services”](#) on page 1794.
  - Write a new `UserRegistry` class that is a DS component and delegate it to your `UserRegistry` class.
  - Register your `UserRegistry` class directly in the Service Registry (SR) using the OSGi core APIs. For more information, see [“Working with the OSGi service registry”](#) on page 1789.
3. Package the custom user registry as an OSGi bundle and export the `UserRegistry` service. For information on creating an OSGi bundle, see [Creating an OSGi service bundle](#).
4. Create a feature manifest to include the OSGi bundle. For more information, see [“Liberty profile: Product extension”](#) on page 967.
5. After the feature is installed into the user product extension location, configure the `server.xml` file with the feature name. For example:

```
<featureManager>
  ...
  <feature>usr:customRegistrySample-1.0</feature>
</featureManager>
```

For a downloadable custom user registry sample, see [https://developer.ibm.com/wasdev/downloads/#asset/samples-Custom\\_User\\_Registry](https://developer.ibm.com/wasdev/downloads/#asset/samples-Custom_User_Registry).

For more information, see <https://www.ibm.com/docs/wasdev/docs/creating-a-custom-user-registry-as-a-liberty-user-feature/>.

## Developing JAAS custom login modules for database authentication

8.5.5.9

You can develop a Java Authentication and Authorization Service (JAAS) custom login module for adding a user name and password to authenticate to a database.

### About this task

You can develop a JAAS custom login module that can be invoked when a database connection that requires authentication is created. The JAAS custom login module is responsible of creating a password credential that contains the user name, password, and managed connection factory. The login module must add the password credential to the subject's private credentials set to be used to authenticate to the database.

### Procedure

1. Create a class that implements the `javax.security.auth.spi.LoginModule` interface.
2. Save the necessary fields in the initialize method. For example:

```
/** {@inheritDoc} */
@SuppressWarnings("unchecked")
@Override
public void initialize(Subject subject, CallbackHandler callbackHandler, Map<String, ?> sharedState, Map<String, ?> o
    this.callbackHandler = callbackHandler;
```

```

    this.subject = subject;
    this.sharedState = (Map<String, Object>) sharedState;
    this.options = options;
}

```

3. Handle the `WSManagedConnectionFactoryCallback` and `WSMappingPropertiesCallback` callbacks in the login method. For example:

```

/** {@inheritDoc} */
@Override
public boolean login() throws LoginException {
    ...
    Callback callbacks[] = new Callback[2];
    callbacks[0] = new WSManagedConnectionFactoryCallback("Target ManagedConnectionFactory: ");
    callbacks[1] = new WSMappingPropertiesCallback("Mapping Properties (HashMap): ");
    callbackHandler.handle(callbacks);
}

```

4. Obtain the managed connection factory and properties in the login method. For example:

```

// The method getManagedConnectionFactory must be used as shown for compatibility with WAS Classic
ManagedConnectionFactory managedConnectionFactory = ((WSManagedConnectionFactoryCallback) callbacks[0]).getManagedConnectionFactory();
Map properties = ((WSMappingPropertiesCallback) callbacks[1]).getProperties();

```

5. Obtain the user name and password based on the authentication data alias or some other criteria. For example:

```

String alias = (String) properties.get(com.ibm.wsspi.security.auth.callback.Constants.MAPPING_ALIAS);
String user = getUser(alias); // Implementation specific
char[] password = getPassword(alias); // Implementation specific

```

6. Create a `javax.resource.spi.PasswordCredential` object with the user name and password and set the managed connection factory. For example:

```

javax.resource.spi.security.PasswordCredential passwordCredential = new PasswordCredential(user, password);
passwordCredential.setManagedConnectionFactory(managedConnectionFactory);

```

7. Add the password credential to the subject in the commit method. For example:

```

/** {@inheritDoc} */
@Override
public boolean commit() throws LoginException {
    // Verify that the login was successful before adding the PasswordCredential to the subject.
    subject.getPrivateCredentials().add(passwordCredential);
    return true;
}

```

## Developing a programmatic login for obtaining authentication data

8.5.5.9

You can use the Java Authentication and Authorization Service (JAAS) login framework to obtain the authentication data from your application.

### About this task

Your application can perform a JAAS programmatic login using the `DefaultPrincipalMapping` JAAS context entry name to obtain a `Subject` object with a `javax.resource.spi.security.PasswordCredential` instance in the private credentials set that contains the user name and password configured for an `authData` element.

### Procedure

1. Add the `appSecurity-2.0`, `passwordUtilities-1.0`, and `jca-1.7` features in the `server.xml` file. You can also add `appSecurity-2.0`, `passwordUtilities-1.0`, and `jca-1.6`. For example:

```

<featureManager>
  <feature>appSecurity-2.0</feature>
  <feature>passwordUtilities-1.0</feature>
  <feature>jca-1.7</feature>
</featureManager>

```

2. Configure an `authData` element in the `server.xml` file. For example:

```
<authData id="myAuthData" user="myUser" password="myPassword"/> <!-- password can also be encoded -->
```

Encode the password within the configuration. You can get the encoded value by using the `securityUtility` `encode` command.

3. Perform a programmatic login with the `DefaultPrincipalMapping` JAAS login context entry name from your application servlet or enterprise bean, replacing the mapping alias with the one you need. For example:

```
HashMap map = new HashMap();
map.put(com.ibm.wsspi.security.auth.callback.Constants.MAPPING_ALIAS, "myAuthData"); // Replace value with your alias
CallbackHandler callbackHandler = new com.ibm.wsspi.security.auth.callback.WSMappingCallbackHandler(map, null);
LoginContext loginContext = new LoginContext("DefaultPrincipalMapping", callbackHandler);
loginContext.login();
Subject subject = loginContext.getSubject();
Set<javax.resource.spi.security.PasswordCredential> creds = subject.getPrivateCredentials(javax.resource.spi.security.PasswordCredential passwordCredential = creds.iterator().next());
```

**Note:** The error handling is not shown for simplicity. A `javax.security.auth.login.LoginException` is returned if the authentication alias requested does not exist or is malformed.

4. Obtain the user name and password from the `PasswordCredential`. For example:

```
String userName = passwordCredential.getUserName();
char[] password = passwordCredential.getPassword();
// Do something with the userName and password.
```

5. If Java 2 Security is enabled, then the application must be granted the `javax.security.auth.PrivateCredentialPermission`. For example, grant the permission in the application's `META-INF/permissions.xml` file to access the `PasswordCredential` object:

```
<?xml version="1.0" encoding="UTF-8"?>
<permissions xmlns="http://xmlns.jcp.org/xml/ns/javaee" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee http://xmlns.jcp.org/xml/ns/javaee/xsi.xsd">

  <permission>
    <class-name>javax.security.auth.PrivateCredentialPermission</class-name>
    <name>javax.resource.spi.security.PasswordCredential * "*"</name>
    <actions>read</actions>
  </permission>

  <!-- Other permissions -->

</permissions>
```

For more information about Java 2 Security, see [Liberty: Java 2 Security](#).

## Developing a custom thread identity service

You can develop a custom thread identity service class by implementing the `com.ibm.wsspi.kernel.security.thread.ThreadIdentityService` interface that is provided in the Liberty server. The `ThreadIdentityService` interface is a Service Programming Interface (SPI) that enables support to receive notifications of user identity switches.

### Procedure

1. Create a custom thread identity service by implementing the `ThreadIdentityService` interface.
2. Convert the implementation class into an OSGi service. You can do the conversion in either of two ways:
  - a. Convert your `ThreadIdentityService` class into a Declarative Service (DS) component. For more information, see “Declaring your services to OSGi Declarative Services” on page 1794.
  - b. Write a new `ThreadIdentityService` class that is a DS component and delegate it to your `ThreadIdentityService` class. Register your `ThreadIdentityService` class directly in the Service Registry (SR) by using the OSGi core APIs. For more information, see “Working with the OSGi service registry” on page 1789.

3. Package the custom thread identity service as an OSGi bundle and export the ThreadIdentityService service. For information on creating an OSGi bundle, see [Creating an OSGi service bundle](#).
4. Create a feature manifest to include the OSGi bundle. For more information, see “Liberty profile: Product extension” on page 967.
5. After the feature is installed into the user product extension location, configure the server.xml file with the feature name.

```
<featureManager>
  ...
  <feature>usr:sampleThreadIdentityService-1.0</feature>
</featureManager>
```

---

## Web services security

### 8.5.5.0

Security is a major quality of service (QoS) requirement for QoS enabled web services. You can provide security for web services in several ways, two of which include transport layer security and message level security.

### Securing web services at the transport layer

Transport-level security is based on a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) and is used to protect HTTP message contents point to point.

### Securing web services at the message level

Message-level security protects the SOAP contents that are contained within an HTTP message for a web service.

## Securing web services at the transport level

### 8.5.5.0

Transport-level security is a well-known and often used mechanism to secure HTTP Internet and intranet communications. Transport-level security can be used to secure web services messages. Transport-level security functionality is independent from functionality that is provided by message-level security (WS-Security) or HTTP basic authentication. You can use the transport-level security binding to secure the communication between your web service client and web service provider.

### Before you begin

The `ibm-ws-bnd.xml` file must be in the `/WEB-INF` directory of a web-based web services application (WAR file), or in the `/META-INF` directory of an EJB-based web service application (JAR file).

**Note:** 8.5.5.6 If the client is running in the Liberty application client container, the `ibm-ws-bnd.xml` file must be in the `/META-INF` directory of the JAR file in the client EAR.

### About this task

Transport-level security is based on Secure Sockets Layer (SSL) or Transport Layer Security (TLS) that runs beneath HTTP.

SSL and TLS provide security features including authentication, data protection, and cryptographic token support for secure HTTP connections. To run with HTTPS, the service port address must be in the form

https://. The integrity and confidentiality of transport data, including SOAP messages and HTTP basic authentication, is confirmed when you use SSL and TLS.

Liberty uses the Java Secure Sockets Extension (JSSE) package to support SSL and TLS. The following security configurations are supported for web services protection in Liberty:

- Secured HTTP
- Basic authentication
- Client certification

For all available elements that you can configure within the `ibm-ws-bnd.xml` file, see “Liberty:The `ibm-ws-bnd.xml` file” on page 2186.

## Procedure

- Enable SSL communications between a web service client and service provider
- Optional: Enable basic authentication between a web service client and service provider
- Optional: Enable client certificate authentication between a web service client and service provider

## Enabling SSL communication for web services access

0.5.5.0

You can configure SSL communication for your client applications to access web services.

### Before you begin

You must complete the following prerequisites before enabling the SSL communication for web services access:

- Generate a pair of self-signed public and private keys for client and provider:

```
keytool -genkey -alias default -keystore myKey.jks -dname "CN=myServer, O=IBM, C=CN"
        -storepass passw0rd -keypass passw0rd -storetype jks -validity 1000 -keyalg RSA
```
- Copy the `myKey.jks` file to the `${server.config.dir}/resources/security` directory of the Liberty server.

**Note:** The `keytool` utility can be found in your Java installation directory.

### About this task

If you need to use your web service client application with the secured HTTP protocol to access the protected web service resources, all the message are encrypted according to the SSL specification.

## Procedure

1. Enable the `jaxws-2.2`, `servlet-3.0`(or `servlet-3.1`) and `appSecurity-2.0` features in the `server.xml` file.

```
<featureManager>
  <feature>jaxws-2.2</feature>
  <feature>servlet-3.0</feature>
  <feature>appSecurity-2.0</feature>
</featureManager>
```

2. Configure the SSL elements in the `server.xml` file.

```
<sslDefault sslRef="customizeSSLConfig" />
<ssl id="customizeSSLConfig" keyStoreRef="serverKeyStore" trustStoreRef="serverTrustStore" />
<keyStore id="serverKeyStore" location="myKey.jks" type="JKS" password="passw0rd" />
<keyStore id="serverTrustStore" location="myKey.jks" type="JKS" password="passw0rd" />
```

3. Configure the service provider by specifying the web service endpoints.

a. Create web services.

```
@WebService(serviceName = "SayHelloPojoService",
             portName = "SayHelloPojoPort")
public class SayHelloPojoService implements SayHelloService {
    ...
}

@WebService(serviceName = "SayHelloStatelessService",
            portName = "SayHelloStatelessPort",
            endpointInterface = "com.ibm.ws.jaxws.transport.server.security.SayHelloService")
@Stateless(name = "SayHelloSessionBean")
public class SayHelloStatelessService implements SayHelloLocal {
    ...
}
```

b. Configure the `ibm-ws-bnd.xml` file for the service provider.

```
<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee
    http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0.xsd "
  version="1.0">
<http-publishing>
<webservice-security>
<security-constraint>
<web-resource-collection>
<web-resource-name>All</web-resource-name>
<url-pattern>*/*/url-pattern>
<http-method>GET</http-method>
<http-method>POST</http-method>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
</webservice-security>
</http-publishing>
</webservices-bnd>
```

**Note:** The `ibm-ws-bnd.xml` file must be in the `/WEB-INF` directory of a web application, or the `/META-INF` directory of a EJB-based web service application (JAR archive).

4. Configure the service client by specifying the web service endpoints. For example, the client application is a web application named `TransportSecurityClient.war`.

a. Configure the client application in the `server.xml` file.

```
<application id="TransportSecurityClient" name="TransportSecurityClient"
  location="TransportSecurityClient.war"
  context-root="TransportSecurityClient" type="war" />
```

b. Configure the `ibm-ws-bnd.xml` file for the client application.

```
<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd id="idvalue0" version="1.0" xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee
    http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0.xsd " >
<!-- POJO service reference binding-->
<service-ref name="service/SayHelloPojoService">
<port name="SayHelloPojoPort"
  namespace="http://ibm.com/ws/jaxws/transport/security/"
  ssl-ref="customizeSSLConfig"/>
<properties http.conduit.tlsClientParameters.disableCNCheck="true" />
</service-ref>
<!-- Stateless service reference binding-->
<service-ref name="service/SayHelloStatelessService">
<port name="SayHelloStatelessPort"
  namespace="http://ibm.com/ws/jaxws/transport/security/"
```

```

        ssl-ref="customizeSSLConfig"/>
        <properties http.conduit.tlsClientParameters.disableCNCheck="true" />
    </service-ref>
</webservices-bnd>

```

**Note:**

- The `ibm-ws-bnd.xml` file must be in the `/WEB-INF` directory of the client web application.
- The value of `ssl-ref` attribute must match the ID value of `ssl` element in `server.xml` file.
- If the `ssl-ref` attribute is not specified in the `ibm-ws-bnd.xml` file, the default SSL configuration in Liberty is used by the web services engine if the configuration is present.
- The `http.conduit.tlsClientParameters.disableCNcheck` attribute is used to control whether to validate the remote server. Use *false* for this attribute in a production environment because the `hostName` verification will be ignored if this attribute is *true*.

c. Generate the client stubs through WSDL location.

```

@WebServiceClient(name = "SayHelloPojoService",
    targetNamespace = "http://ibm.com/ws/jaxws/transport/security/",
    wsdlLocation = "https://localhost:8020/TransportSecurityProvider/Unauthorized/employPojoService?wsdl")
public class SayHelloPojoService
    extends Service
{...}

@WebServiceClient(name = "SayHelloStatelessService",
    targetNamespace = "http://ibm.com/ws/jaxws/transport/security/",
    wsdlLocation = "https://localhost:8020/TransportSecurityProvider/Unauthorized/EmployStatelessService?wsdl")
public class SayHelloStatelessService
    extends Service
{...}

```

d. Use the `@WebServiceRef` annotation to inject the web service into the servlet. For example, the `TestJaxWsTransportSecurityServlet`.

```

@WebServiceRef(name = "service/SayHelloPojoService")
SayHelloPojoService pojoService;

@WebServiceRef(name = "service/SayHelloStatelessService")
SayHelloStatelessService statelessService;

```

## Enabling basic authentication for web services access

**8.5.5.0**

You can configure basic authentication for your client applications to access web services.

### About this task

If you need to use your web service client application with the basic authentication to access the protected web service resources, the client must provide the user name and password in the request when communicating with the service provider.

### Procedure

1. Enable the `jaxws-2.2`, `servlet-3.0`(or `servlet-3.1`) and `appSecurity-2.0` features in the `server.xml` file.

```

<featureManager>
    <feature>jaxws-2.2</feature>
    <feature>servlet-3.0</feature>
    <feature>appSecurity-2.0</feature>
</featureManager>

```

2. Configure the login realm in the `server.xml` file and bind the realm to the service provider.

```

<application id="TransportSecurityProvider" name="TransportSecurityProvider"
    location="TransportSecurityProvider.war" type="ear">
    <application-bnd>
        <security-role name="Employee">

```

```

        <user name="employee0" />
        <group name="employeeGroup" />
    </security-role>
    <security-role name="Manager">
        <user name="manager0" />
    </security-role>
    <security-role name="AllAuthenticated">
        <special-subject type="ALL_AUTHENTICATED_USERS" />
    </security-role>
</application-bnd>
</application>

<basicRegistry id="basic" realm="BasicRealm">
    <user name="employee0" password="emp0pwd" />
    <user name="employee1" password="emp1pwd" />
    <user name="manager0" password="mgr0pwd" />
    <group name="employeeGroup">
        <member name="employee0" />
        <member name="employee1" />
    </group>
</basicRegistry>

```

### 3. Configure the service provider by specifying the web service endpoints.

#### a. Create web services.

```

@WebService(serviceName = "SayHelloPojoService",
            portName = "SayHelloPojoPort")
public class SayHelloPojoService implements SayHelloService {
    ...
}

@WebService(serviceName = "SayHelloStatelessService",
            portName = "SayHelloStatelessPort",
            endpointInterface = "com.ibm.ws.jaxws.transport.server.security.SayHelloService")
@Stateless(name = "SayHelloSessionBean")
public class SayHelloStatelessService implements SayHelloLocal {
    ...
}

```

#### b. Configure the ibm-ws-bnd.xml file for the service provider.

```

<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0.xsd"
    version="1.0">
<http-publishing>
<webservice-security>
<security-constraint>
<web-resource-collection>
<web-resource-name>Only Managers</web-resource-name>
<url-pattern>/manager/*</url-pattern>
<http-method>GET</http-method>
<http-method>POST</http-method>
</web-resource-collection>
<auth-constraint id="AuthConstraint_manager">
<role-name>Manager</role-name>
</auth-constraint>
</security-constraint>
<security-constraint>
<web-resource-collection>
<web-resource-name>Employees</web-resource-name>
<url-pattern>/employee/*</url-pattern>
<http-method>GET</http-method>
<http-method>POST</http-method>
</web-resource-collection>
<auth-constraint id="AuthConstraint_employee">
<role-name>Employee</role-name>
</auth-constraint>
</security-constraint>
<!-- SECURITY ROLES -->
<security-role id="Staff">
<role-name>Employee</role-name>

```

```

    <role-name>Manager</role-name>
  </security-role>
  <!-- AUTHENTICATION METHOD: Basic authentication -->
  <login-config id="LoginConfig">
    <auth-method>BASIC</auth-method>
    <realm-name>Authentication</realm-name>
  </login-config>
</webservice-security>
</http-publishing>
</webservices-bnd>

```

**Note:**

- The `ibm-ws-bnd.xml` file must be in the `/WEB-INF` directory of a web application, or the `/META-INF` directory of an EJB-based web service application (JAR archive).
- The `login-config` element in the `ibm-ws-bnd.xml` file takes effect only in an EJB-based web service application (JAR archive). For a web application, the `login-config` element is ignored and the value of the same element in the `web.xml` file is used.

4. Configure the service client by specifying the web service endpoints. For example, the client application is a web application named `TransportSecurityClient.war`.

a. Configure the client application in the `server.xml` file.

```

<application id="TransportSecurityClient" name="TransportSecurityClient"
  location="TransportSecurityClient.war"
  context-root="TransportSecurityClient" type="war" />

```

b. Configure the `ibm-ws-bnd.xml` file for the client application.

```

<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0.xsd"
  version="1.0">
  <!-- POJO service reference binding-->
  <service-ref name="service/SayHelloPojoService">
    <port name="SayHelloPojoPort"
      namespace="http://ibm.com/ws/jaxws/transport/security/"
      username="employee1"
      password="{xor}0jIvbi8o0w=="
    />
  </service-ref>
  <!-- Stateless service reference binding-->
  <service-ref name="service/SayHelloStatelessService">
    <port name="SayHelloStatelessPort"
      namespace="http://ibm.com/ws/jaxws/transport/security/"
      username="employee1"
      password="{xor}0jIvbi8o0w=="
    />
  </service-ref>
</webservices-bnd>

```

**Note:**

- The `ibm-ws-bnd.xml` file must be in the `/WEB-INF` directory of the client web application.
- The values of **username** and **password** attributes must match the user name and password of `basicRegistry` element in `server.xml` file. The password can be encoded by using the `securityUtility` command.

c. Generate the client stubs by using the `wsdl` location.

```

@WebServiceClient(name = "SayHelloPojoService",
  targetNamespace = "http://ibm.com/ws/jaxws/transport/security/",
  wsdlLocation = "https://localhost:8020/TransportSecurityProvider/authorized/employPojoService?wsdl")
public class SayHelloPojoService
  extends Service
{...}

@WebServiceClient(name = "SayHelloStatelessService",
  targetNamespace = "http://ibm.com/ws/jaxws/transport/security/",
  wsdlLocation = "https://localhost:8020/TransportSecurityProvider/authorized/EmployStatelessService?wsdl")
public class SayHelloStatelessService
  extends Service
{...}

```

- d. Use the `@WebServiceRef` annotation to inject the web service into the servlet. For example, the `TestJaxWsTransportSecurityServlet`.

```
@WebServiceRef(name = "service/SayHelloPojoService")
SayHelloPojoService pojoService;

@WebServiceRef(name = "service/SayHelloStatelessService")
SayHelloStatelessService statelessService;
```

## Enabling client certificate authentication for web services access

0.5.5.0

You can configure client certificate authentication for your client applications to access web services.

### Before you begin

You must complete the following prerequisites before enabling client certificate authentication for web services access:

- Generate a pair of self-signed public and private keys for provider.  

```
keytool -genkey -alias default -keystore serverKey.jks -dname "CN=myServer, O=IBM, C=CN"
-storepass passw0rd -keypass passw0rd -storetype jks -validity 1000 -keyalg RSA
```
- Export the certificate of the default and import the certificate into the trust store.  

```
keytool -export -alias default -file myserver.cer -keystore serverKey.jks
-storepass passw0rd -storetype jks
keytool -import -file myserver.cer -alias default -keystore clientTrust.jks
-storepass passw0rd -keypass passw0rd -storetype jks
```
- Generate two pairs of self-signed public and private for client.  

```
keytool -genkey -alias user0 -keystore clientKey.jks -dname "CN=employee0, O=IBM, C=CN"
-storepass passw0rd -keypass passw0rd -storetype jks -validity 1000 -keyalg RSA
keytool -genkey -alias admin0 -keystore clientKey.jks -dname "CN=manager0, O=IBM, C=CN"
-storepass passw0rd -keypass passw0rd -storetype jks -validity 1000 -keyalg RSA
```
- Export the certificates of the two alias and import the certificate into the trust store.  

```
keytool -export -alias user0 -file user0.cer -keystore clientKey.jks -storepass passw0rd -storetype jks
keytool -export -alias admin0 -file admin0.cer -keystore clientKey.jks -storepass passw0rd -storetype jks
keytool -import -file user0.cer -alias user0 -keystore serverTrust.jks -storepass passw0rd -keypass passw0rd -storetype jks
keytool -import -file admin0.cer -alias admin0 -keystore serverTrust.jks -storepass passw0rd -keypass passw0rd -storetype jks
```
- Copy the `serverKey.jks`, `serverTrust.jks`, `clientKey.jks`, and `clientTrust.jks` files to the `${server.config.dir}/resources/security` directory.

**Note:** The `keytool` utility can be found in your Java installation directory.

### About this task

If you need to use the web service client application with the Client Certificate Authentication to access the protected web service resources, the client must provide the valid certificate in the request and must use the HTTPS to communicate with the service provider.

### Procedure

1. Enable the `jaxws-2.2`, `servlet-3.0`(or `servlet-3.1`) and `appSecurity-2.0` features in the `server.xml` file.  

```
<featureManager>
  <feature>jaxws-2.2</feature>
  <feature>servlet-3.0</feature>
  <feature>appSecurity-2.0</feature>
</featureManager>
```
2. Configure the SSL element and client customized SSL element in the `server.xml` file.

```

<!-- Server SSL configuration -->
<ssl id="defaultSSLConfig" keyStoreRef="serverKeyStore" trustStoreRef="serverTrustStore"
  clientAuthenticationSupported="true"/>
<keyStore id="serverKeyStore" location="serverKey.jks" type="JKS" password="passw0rd" />
<keyStore id="serverTrustStore" location="serverTrust.jks" type="JKS" password="passw0rd" />

<!-- customize SSL configuration -->
<ssl id="customizeSSLConfig" keyStoreRef="clientKeyStore" trustStoreRef="clientTrustStore" />
<keyStore id="clientKeyStore" location="clientKey.jks" type="JKS" password="passw0rd" />
<keyStore id="clientTrustStore" location="clientTrust.jks" type="JKS" password="passw0rd" />

```

### 3. Configure the login realm in the server.xml file and bind the realm to the service provider.

```

<application id="TransportSecurityProvider" name="TransportSecurityProvider"
  location="TransportSecurityProvider.war" type="ear">
  <application-bnd>
    <security-role name="Employee">
      <user name="employee0" />
      <group name="employeeGroup" />
    </security-role>
    <security-role name="Manager">
      <user name="manager0" />
    </security-role>
    <security-role name="AllAuthenticated">
      <special-subject type="ALL_AUTHENTICATED_USERS" />
    </security-role>
  </application-bnd>
</application>

<basicRegistry id="basic" realm="BasicRealm">
  <user name="employee0" password="emp0pwd" />
  <user name="employee1" password="emplpwd" />
  <user name="manager0" password="mgr0pwd" />
  <group name="employeeGroup">
    <member name="employee0" />
    <member name="employee1" />
  </group>
</basicRegistry>

```

### 4. Configure the service provider.

#### a. Create web services.

```

@WebService(serviceName = "SayHelloPojoService",
  portName = "SayHelloPojoPort")
public class SayHelloPojoService implements SayHelloService {
  ...
}

@WebService(serviceName = "SayHelloStatelessService",
  portName = "SayHelloStatelessPort",
  endpointInterface = "com.ibm.ws.jaxws.transport.server.security.SayHelloService")
@Stateless(name = "SayHelloSessionBean")
public class SayHelloStatelessService implements SayHelloLocal {
  ...
}

```

#### b. Configure the ibm-ws-bnd.xml file for the service provider.

```

<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0.xsd"
  version="1.0">

<http-publishing>
<webservice-security>
<security-constraint>
<web-resource-collection>
  <web-resource-name>Only Managers</web-resource-name>
  <url-pattern>/manager/*</url-pattern>
  <http-method>GET</http-method>

```

```

    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint id="AuthConstraint_manager">
    <role-name>Manager</role-name>
  </auth-constraint>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Employees</web-resource-name>
    <url-pattern>/employee/*</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint id="AuthConstraint_employee">
    <role-name>Employee</role-name>
  </auth-constraint>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
<!-- SECURITY ROLES -->
<security-role id="Staff">
  <role-name>Employee</role-name>
  <role-name>Manager</role-name>
</security-role>
<!-- AUTHENTICATION METHOD: client-cert authentication -->
<!-- login configuration -->
<login-config id="LoginConfig">
  <auth-method>CLIENT-CERT</auth-method>
  <realm-name>Authentication</realm-name>
</login-config>
</webservice-security>
</http-publishing>
</webservices-bnd>

```

**Note:**

- The `ibm-ws-bnd.xml` file must be in the `/WEB-INF` directory of a web application, or the `/META-INF` directory of an EJB-based web service application (JAR archive).
- The `login-config` element in the `ibm-ws-bnd.xml` file takes effect only in an EJB-based web service application (JAR archive). For a web application, the `login-config` element is ignored and the value of the same element in the `web.xml` file is used.

5. Configure the service client by specifying the web service endpoints. For example, the client application is a web application named `TransportSecurityClient.war`.

a. Configure the client application in the `server.xml` file.

```

<application id="TransportSecurityClient" name="TransportSecurityClient"
  location="TransportSecurityClient.war"
  context-root="TransportSecurityClient" type="war" />

```

b. Configure the `ibm-ws-bnd.xml` file for the client application.

```

<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0.xsd"
  version="1.0">
  <!-- POJO service reference binding-->
  <service-ref name="service/SayHelloPojoService">
    <port name="SayHelloPojoPort"
      namespace="http://ibm.com/ws/jaxws/transport/security/"
      ssl-ref="customizeSSLConfig"
      key-alias="user0"/>
    <properties http.conduit.tlsClientParameters.disableCNCheck="true" />
  </service-ref>
  <!-- Stateless service reference binding-->
  <service-ref name="service/SayHelloStatelessService">
    <port name="SayHelloStatelessPort"
      namespace="http://ibm.com/ws/jaxws/transport/security/"
      ssl-ref="customizeSSLConfig"

```

```

    key-alias="user0"/>
    <properties http.conduit.tlsClientParameters.disableCNCheck="true" />
  </service-ref>
</webservices-bnd>

```

#### Note:

- The `ibm-ws-bnd.xml` file must be in the `/WEB-INF` directory of the client web application.
- The **key-alias** attribute specifies the valid client certificate in client key store that is defined in the `server.xml` file. In this example, the client keystore is defined as follows:
 

```
<keyStore id="clientKeyStore" location="clientKey.jks" type="JKS" password="passw0rd" />
```
- The **ssl-ref** attribute in the `ibm-ws-bnd.xml` file must match the correct **id** attribute of the `ssl` element in the `server.xml` file. In this example, the `ssl` element is defined as follows:
 

```
<ssl id="customizeSSLConfig" keyStoreRef="clientKeyStore" trustStoreRef="clientTrustStore" />
```
- The value of **key-alias** attribute can also override the value of **clientKeyAlias** attribute of the `ssl` element in the `server.xml` file.

#### c. Generate the client stubs through WSDL location.

```

@WebServiceClient(name = "SayHelloPojoService",
    targetNamespace = "http://ibm.com/ws/jaxws/transport/security/",
    wsdlLocation = "https://localhost:8020/TransportSecurityProvider/unauthorized/employPojoService?wsdl")
public class SayHelloPojoService
    extends Service
{...}

@WebServiceClient(name = "SayHelloStatelessService",
    targetNamespace = "http://ibm.com/ws/jaxws/transport/security/",
    wsdlLocation = "https://localhost:8020/TransportSecurityProvider/unauthorized/EmployStatelessService?wsdl")
public class SayHelloStatelessService
    extends Service
{...}

```

- d. Use the `@WebServiceRef` annotation to inject the web service into the servlet. For example, the `TestJaxWsTransportSecurityServlet`.

```

@WebServiceRef(name = "service/SayHelloPojoService")
SayHelloPojoService pojoService;

@WebServiceRef(name = "service/SayHelloStatelessService")
SayHelloStatelessService statelessService;

```

## Web Services Security at the message level

### 8.5.5.0

Web services message level security (Web Services Security or WS-Security) is a security quality of service (QoS) for web services applications. WS-Security standards and profiles describe how to provide security and protection for SOAP messages that are exchanged in a web services environment.

### 8.5.5.0

WS-Security is provided as a Liberty feature. The WS-Security run time that is provided in Liberty is based on the Apache CXF open source services framework. The WS-Security feature in Liberty is limited by the features and function of the Apache CXF framework. WS-Security must be explicitly enabled by enabling the `wsSecurity-1.1` feature. Make sure you also add the `appSecurity-2.0`, `servlet-3.0`(or `servlet-3.1`) and `jaxws-2.2` features, and other required Liberty features to the `server.xml` file of the Liberty.

WS-Security is configured by using the `WS-SecurityPolicy` within the WSDL file of a web service application. To protect your web service application with WS-Security, your JAX-WS application must contain a `wsdl` that has an embedded WS-Security policy. There must be a `PolicyReference` to the embedded WS-Security policy in either the `wsdl:binding` or `wsdl:operation` sections or both.

## Web Services Security specifications and standards

### 8.5.5.0

Liberty supports a number of Organization for the Advancement of Structured Information Standards (OASIS) standards.

- Web Services Security SOAP Message Security 1.1: <http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>
- Web Services Security Username Token Profile 1.1: <http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-UsernameTokenProfile.pdf>
- Web Services Security X.509 Certificate Token Profile 1.1: <http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-x509TokenProfile.pdf>
- WS-SecurityPolicy 1.3: <http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/os/ws-securitypolicy-1.3-spec-os.pdf>

## WS-Security behavior differences between traditional and Liberty

### 8.5.5.0

The WS-Security constraints that can be added to a web service application in Liberty may behave differently from the same constraints applied to a service in traditional.

### WS-Security enablement and configuration

WS-Security in Liberty is configured by using the WS-SecurityPolicy within the WSDL file of a web service application, and is enabled by adding the wsSecurity-1.1 feature in the server.xml file.

WS-Security in traditional is configured by using a policysset and enabled by attaching a policysset. If you deploy a WS-Security enabled Liberty web service application to traditional, you must create and attach an equivalent policysset and bindings to get the same level of web service security.

### WS-Security Policy

- Namespaces
  - The Liberty CXF WS-Security supports the following WS-Security Policy namespaces:  
<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702>  
<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200802>
  - The following namespace is also supported, with limitations:  
<http://schemas.xmlsoap.org/ws/2005/07/securitypolicy>
  - The WS-Security of traditional supports the following WS-Security Policy namespaces:  
<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512>

- Assertions

Liberty supports more assertions in the WS-Security Policy 1.2 than traditional. Some policy assertions in traditional WS-Security are implemented through XPath or bindings. The following list shows some important differences:

- Supporting Tokens

To sign or encrypt a SupportingToken such as a UsernameToken in Liberty, you assert the token as SignedSupportingTokens, SignedEncryptedSupportingTokens, or EncryptedSupportingTokens. In traditional, you must use an XPath expression to sign or encrypt a SupportingToken.

All endorsing tokens are not supported in traditional, including EndorsingSupportingTokens, SignedEndorsingSupportingTokens, EndorsingEncryptedSupportingTokens, and SignedEndorsingEncryptedSupportingTokens.

- Security Binding Assertion

Liberty supports the SymmetricBinding, AsymmetricBinding, and TransportBinding assertions. The traditional application server does not support the TransportBinding assertion.

- IncludeToken Assertion

The IncludeToken assertion is enforced in Liberty, but is ignored in the WS-Security runtime environment of traditional.

- UsernameToken Assertion

Liberty supports PasswordDigest and key derivation in the UsernameToken assertion. The traditional application server supports only PasswordText in a UsernameToken.

## Unrecognized elements in the Security headers

- An unrecognized element in the Security header is rejected by traditional, while it is accepted by Liberty.

## Encrypted header

- The WS-Security 1.1 specification recommends using the <wsse11:EncryptedHeader> element for encrypting SOAP header blocks.
  - The CXF WS-Security that is used in Liberty does not generate an EncryptedHeader element. Instead, the CXF WS-Security generates an <xenc:EncryptedData> element. However, the CXF WS-Security that is used in Liberty can process and consume an incoming <wsse11:EncryptedHeader> element if mustUnderstand in the <security> header is set to 0.
  - The WebSphere Application Server traditional always sets mustUnderstand to 1 in the <security> header. In order for Liberty to process the EncryptedHeader element successfully, you must explicitly set mustUnderstand to 0 by setting the following property in the outbound bindings configuration:  
`<properties name="com.ibm.wsspi.wssecurity.config.request.setMustUnderstand" value="false"/>`

## Intermediate non-trusted certificates

- There is no way to specify intermediate non-trusted certificates to allow the certificate path validator to build a certificate path from an inbound certificate to a trusted certificate in a trust store. Either the inbound certificate or its immediate issuer must be in the trust store for the certificate to be trusted.

## Known issues

- There are some known issues in Liberty CXF WS-Security. Some of the issues have work-arounds. To find known issues and work-arounds, see WS-Security known issues and work-arounds.

## Not tested and not supported features

- Liberty WS-Security includes all of the WS-Security runtime environment code from the CXF project. However, not all functions and features in the CXF WS-Security were tested or verified. To see a list of the specifications that were not verified, see Untested WS-Security specifications.

## WS-Security known issues and work-arounds: **8.5.5.0**

The following items are issues with the WS-Security implementation in the Apache CXF open source services framework.

- If your SupportingToken is being encrypted when you intended to encrypt nothing, try removing any encryption-related token assertions to resolve the issue. If there are no EncryptedParts and no EncryptedElements in an AsymmetricBinding with SupportingToken assertion, then the SupportingToken is encrypted unexpectedly.
- XML Signature with Enveloped Signature Transformation does not work. There is no work-around.
- Although the PolicyReference within <wsdl:output> is honored, the PolicyReference within <wsdl:input> is ignored. If you must distinguish PolicyReference between input and output, the work-around is to attach PolicyReference at the binding level and then override PolicyReference in <wsdl:output>.
- sp:requireEmbeddedTokenReference policy assertion is not supported.

- When the `org.apache.ws.security.crypto.merlin.truststore.*` properties exist in the `signatureProperties` element and the `org.apache.ws.security.crypto.merlin.keystore.*` properties exist in the `encryptProperties` element in the `wsSecurityProvider` or `wsSecurityClient` section of the `server.xml` file, the `org.apache.ws.security.crypto.merlin.keystore.*` values in the `encryptProperties` element overrides the `org.apache.ws.security.crypto.merlin.truststore.*` properties in the `signatureProperties` element. This behavior means that your encryption keystore is used for your signature trust store. The work-around is to use the same keystore for both encryption and signature trust store; separate keystores cannot be used.
- The `X509PKIPathv1` and `PKCS#7` token types are not supported.
- In the WS-Security policy, the `Require*` assertions within the `X509Token` assertion are only used when generating an X509 token. They are not enforced when consuming an X509 token. These assertions include, but are not limited to, `RequireKeyIdentifierReference`, `RequireIssuerSerialReference`, and `RequireThumbprintReference`.
- In the `SymmetricBinding` assertion, neither the `SignatureToken` nor the `EncryptionToken` assertions can be specified. The only supported assertion that can be used within a `SymmetricBinding` assertion is the `ProtectionToken` assertion. The `ProtectionToken` specified is used for both signature and encryption.
- The `ProtectTokens` assertion in the WS-Security policy is not supported and is ignored.
- The `KeyValueToken` assertion in the WS-Security policy is not supported.
- `X509Token` within `EndorsingEncryptedSupportingTokens` or `SignedEndorsingEncryptedSupportingTokens` is not supported.
- WS-Security in Liberty supports the version 1.1 specification, which is compatible with an earlier version with the version 1.0 specification. This means that URIs and schema elements that are defined in 1.0 remain unchanged, while new schema elements and constants are defined with 1.1 namespaces and URIs.

WS-Security options and properties in the WS-Security policy is defined with the `wss10` assertion or the `wss11` assertion. If you must configure a policy to support the WS-Security 1.1 properties, you must configure only the `wss11` policy assertion that already includes the `wss10` assertion, and you must not configure both the `wss11` and the `wss10` policy assertions.

Examples of `wss11` policy assertions that contain the `wss10` assertion include, but are not limited to, `RequireSignatureConfirmation`, `MustSupportRefKeyIdentifier` and `MustSupportRefIssuerSerial`.

- WS-Security and MTOM cannot be configured together for the same service at this time. When MTOM is used and WS-Security is also configured, the SOAP message is not sent properly. The user must make a choice to either use MTOM or configure WS-Security. If MTOM is required, you must remove the WS-Security policy from the WSDL file to disable WS-Security.
- If you are using a Liberty profile client and a WebSphere Application Server traditional provider and receive a `CWWS6001E: Key object was not obtained.` response from the provider, the issue might be resolved by WebSphere Application Server traditional APAR PM88011. This issue specifically relates to configurations that include both asymmetric digital signature and encryption of the Body.

**Untested WS-Security specifications:** **8.5.5.0** The following list of specifications are not verified. However, this list does not include all specifications that are not yet verified.

1. Web Services Security SAML Token Profile 1.1: <http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLSAMLTokenProfile.pdf>
2. Web Services Security Kerberos Token Profile 1.1: <http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-KerberosTokenProfile.pdf>
3. WS-SecureConversation 1.3: <http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.html>
4. WS-Trust 1.3: <http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html>

## Web Services Security default configuration

**8.5.5.0**

A Web Services Security (WS-Security) configuration is complementary to the WS-Security policy at run time. The WS-Security configuration follows the CXF name and value pair style, and preserves the CXF property name. Some of the properties have default values and some do not.

In the `server.xml` file, the WebSphere Application Server Liberty profile provides a server-level configuration that is applied to all services. This configuration is known as the default WS-Security configuration.

The `server.xml` file has two default WS-Security configurations: one for client applications and one for provider applications. No other WS-Security configurations can exist in the `server.xml` file. If you need a custom WS-Security configuration for your application that deviates from the default, the configuration must be done programmatically.

The following example shows a default client configuration:

```
<wsSecurityClient id="default"
  ws-security.username="user2"
  ws-security.password="security">
  <signatureProperties org.apache.ws.security.crypto.merlin.keystore.type="jks"
    org.apache.ws.security.crypto.merlin.keystore.password="LibertyX509Client"
    org.apache.ws.security.crypto.merlin.keystore.alias="x509ClientCert"
    org.apache.ws.security.crypto.merlin.file="{server.config.dir}/x509ClientDefault.jks"/>
</wsSecurityClient>
```

The following example shows a default provider configuration:

```
<wsSecurityProvider id="default"
  ws-security.username="user2">
  <encryptionProperties org.apache.ws.security.crypto.merlin.keystore.type="jks"
    org.apache.ws.security.crypto.merlin.keystore.password="LibertyX509Server"
    org.apache.ws.security.crypto.merlin.keystore.alias="x509ServerCert"
    org.apache.ws.security.crypto.merlin.file="{server.config.dir}/x509ServerDefault.jks"/>
</wsSecurityProvider>
```

The following table shows the default WS-Security user properties in Liberty. These same properties can be found in CXF.

*Table 137. Default WS-Security user properties in Liberty and CXF*

Liberty profile/CXF property	Default value
<code>ws-security.username</code>	none
<code>ws-security.password</code>	none
<code>ws-security.signature.username</code>	none
<code>ws-security.encryption.username</code>	none

The following table shows the WS-Security callback handler class and crypto properties in Liberty and the equivalent CXF properties, if different.

*Table 138. WS-Security callback handler class and crypto properties in Liberty and the equivalent CXF properties*

Liberty profile property	CXF property	Default value
<code>ws-security.callback-handler</code>		none
<code>&lt;signatureProperties&gt;</code>	<code>ws-security.signature.properties</code>	none
<code>&lt;encryptionProperties&gt;</code>	<code>ws-security.encryption.properties</code>	none

In the WebSphere Application Server, the `wss4j` properties are specified as attributes of the `signatureProperties` or `encryptionProperties` elements. The following example shows the `wss4j` properties:

```

<signatureProperties org.apache.ws.security.crypto.merlin.keystore.type="jks"
                    org.apache.ws.security.crypto.merlin.keystore.password="LibertyX509Client"
                    org.apache.ws.security.crypto.merlin.keystore.alias="x509ClientDefault"
                    org.apache.ws.security.crypto.merlin.file="${server.config.dir}/x509ClientDefault.jks">
</signatureProperties>

```

The following table shows the wss4j crypto properties in Liberty. These same properties can be found in CXF.

*Table 139. wss4j crypto properties in Liberty and CXF*

Liberty profile/CXF property	Default value
org.apache.ws.security.crypto.provider	org.apache.ws.security.components.crypto.Merlin
org.apache.ws.security.crypto.merlin.keystore.provider	defaults to the installed provider
org.apache.ws.security.crypto.merlin.cert.provider	defaults to the keystore provider
org.apache.ws.security.crypto.merlin.x509crl.file	none

The following table shows the wss4j keystore properties in Liberty. These same properties can be found in CXF.

*Table 140. wss4j keystore properties in Liberty and CXF*

Liberty profile/CXF property	Default value
org.apache.ws.security.crypto.merlin.keystore.file	none
org.apache.ws.security.crypto.merlin.keystore.password	none
org.apache.ws.security.crypto.merlin.keystore.type	none
org.apache.ws.security.crypto.merlin.keystore.alias	none
org.apache.ws.security.crypto.merlin.keystore.private.password	none

The following table shows the wss4j truststore properties in Liberty. These same properties can be found in CXF.

*Table 141. wss4j truststore properties in Liberty and CXF*

Liberty profile property	Default value
org.apache.ws.security.crypto.merlin.truststore.file	none
org.apache.ws.security.crypto.merlin.truststore.password	none
org.apache.ws.security.crypto.merlin.truststore.type	none

The following table shows the WS-Security miscellaneous properties in Liberty. These same properties can be found in CXF.

*Table 142. WS-Security miscellaneous properties in Liberty and CXF*

Liberty profile/CXF property	Default value
ws-security.enable.nonce.cache	true
ws-security.cache.config.file	none

The following table shows the properties that are supported only in Liberty.

Table 143. Properties that are supported only in Liberty

Liberty profile property	CXF property	Default value
callerToken	none	none

## Configuring additional properties

You can set several extra properties to provide additional configuration information to the WS-Security runtime environment. See the following links for detailed information regarding these properties:

- <http://cxf.apache.org/docs/ws-securitypolicy.html>
- <http://ws.apache.org/wss4j/config.html>

Any of the additional properties can be specified in the default WS-Security configuration in the `server.xml` file.

For example, to specify any additional properties, specify them in either the `wsSecurityClient` or `wsSecurityProvider` sections, or both.

```
<wsSecurityProvider id="default"
  <signatureProperties ... />
  <encryptionProperties ... />
  ws-security.cache.config.file = "${server.config.dir}/resources/ws-security/new_cxf-ehcache.xml"
</wsSecurityProvider>

<wsSecurityClient id="default"
  <signatureProperties ... />
  <encryptionProperties ... />
  ws-security.username-token.always.encrypted="false"
</wsSecurityClient>
```

## Configuring cache

WS-Security provides a default caching implementation for nonce in a UsernameToken, the created Timestamp, and security tokens. The default cache implementation is based on ehCache with the following default settings:

```
maxEntriesLocalHeap="5000"
timeToIdleSeconds="3600"
timeToLiveSeconds="3600"
overflowToDisk="true"
maxElementsOnDisk="10000000"
diskPersistent="false"
diskExpiryThreadIntervalSeconds="120"
memoryStoreEvictionPolicy="LRU"
```

To modify the default cache settings, you can provide an ehCache configuration XML file. Use the `ws-security.cache.config.file` custom property to specify a file name with customized properties to deviate from the default settings. You must put this file somewhere in the server profile. You can find an additional sample cache setting configuration file from <http://svn.apache.org/viewvc/cxf/trunk/rt/ws/security/src/main/resources/cxf-ehcache.xml?view=markup>.

## Configuring a stronger signature algorithm

Because of the weakness of the SHA1 signature algorithm, the US National Institute of Standards and Technology (NIST) recommends that you use stronger signature algorithms.

However, WS-Security policy 1.3 defines HmacSha1 or RsaSha1 (collectively called sha1) as the only signature algorithm. WS-Security in Liberty has a configuration option to use the following stronger signature algorithm:

- RSA-SHA-256
- RSA-SHA-384
- RSA-SHA-512
- HMAC-SHA-256
- HMAC-SHA-384
- HMAC-SHA-512

To configure WS-Security in Liberty to support the stronger signature algorithm, you use the `signatureAlgorithm` attribute to define the required algorithm within the `<signatureProperties>` element in the `server.xml` file. The valid values for the `signatureAlgorithm` attribute are `sha256`, `sha384`, and `sha512`. For example, if you specify `sha512` as the value of the `signatureAlgorithm` attribute, the signature algorithm that is used in the signature with an asymmetric key is RSA-SHA-512, and the signature algorithm that is used in the signature with a symmetric key is HMAC-SHA-512.

The following example shows a sample client side configuration that requires the `sha256` signature algorithm:

```
<wsSecurityClient id="default"
  ws-security.password="security"
  ws-security.username="user1"
  ws-security.callback-handler="com.ibm.ws.wssecurity.example.cbh.CommonPasswordCallback"
  ws-security.signature.username="soaprequester">
  <signatureProperties
    signatureAlgorithm="sha256"
    org.apache.ws.security.crypto.merlin.keystore.type="jks"
    org.apache.ws.security.crypto.merlin.keystore.password="client"
    org.apache.ws.security.crypto.merlin.keystore.alias="soaprequester"
    org.apache.ws.security.crypto.merlin.file="${server.config.dir}/dsig-sender.ks" />
</wsSecurityClient>
```

The following example shows a sample provider side configuration that requires the `sha256` signature algorithm:

```
<wsSecurityProvider id="default"
  ws-security.callback-handler="com.ibm.ws.wssecurity.example.cbh.CommonPasswordCallback"
  ws-security.signature.username="soapprovider">
  <signatureProperties
    signatureAlgorithm="sha256"
    org.apache.ws.security.crypto.merlin.keystore.type="jks"
    org.apache.ws.security.crypto.merlin.keystore.password="server"
    org.apache.ws.security.crypto.merlin.keystore.alias="soapprovider"
    org.apache.ws.security.crypto.merlin.file="${server.config.dir}/dsig-receiver.ks" />
</wsSecurityProvider>
```

## Authentication of web services clients with a UsernameToken

### 8.5.5.0

The WebSphere Application Server Liberty profile supports the OASIS Web Services Security UsernameToken Profile 1.1 specification. The specification describes how a web services client supplies a UsernameToken as a means of identifying the requestor by using a user name, and optionally by using a password or password-equivalent to the web services provider. The Web Services Security (WS-Security) run time in Liberty that processes the policy for the web services provider can use this identifying information to authenticate the user.

The requirement of a UsernameToken is expressed as one of the supporting tokens in the WS-Security policy. You can add a UsernameToken requirement as a required token in one of supporting token assertions, including `SupportingTokens`, `SignedSupportingTokens`, `SignedEndorsingSupportingTokens`, `SignedEncryptedSupportingTokens`, and `EncryptedSupportingTokens`.

The following example shows a sample policy fragment that requires a UsernameToken with password text to be sent in the Security header of a SOAP message to a web services provider:

```

<sp:SupportingTokens>
  <wsp:Policy>
    <sp:UsernameToken
      sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
      <wsp:Policy>
        <sp:WssUsernameToken11 />
      </wsp:Policy>
    </sp:UsernameToken>
  </wsp:Policy>
</sp:SupportingTokens>

```

In addition to the requirement of providing a user name or a password, you can configure a policy to include a nonce and created timestamp in a UsernameToken.

The following example shows a sample policy fragment that requires a UsernameToken with password text, nonce, and created timestamp to be sent in the Security header of a SOAP message to a web services provider:

```

<sp:SupportingTokens>
  <wsp:Policy>
    <sp:UsernameToken
      sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
      <wsp:Policy>
        <sp:WssUsernameToken11 />
        <sp13:Created />
        <sp13:Nonce />
      </wsp:Policy>
    </sp:UsernameToken>
  </wsp:Policy>
</sp:SupportingTokens>

```

The following example shows a sample policy fragment that requires a UsernameToken with password digest instead of password text:

```

<sp:SupportingTokens>
  <wsp:Policy>
    <sp:UsernameToken
      sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
      <wsp:Policy>
        <sp:WssUsernameToken11 />
        <sp:HashPassword />
      </wsp:Policy>
    </sp:UsernameToken>
  </wsp:Policy>
</sp:SupportingTokens>

```

For more information about nonce, created, and different password types, see the OASIS WS-Security policy 1.3 specification.

## Providing a user name and password in a web services client

The WS-Security feature in Liberty provides more than one method for indicating the user name and password for a client application when generating a UsernameToken. You can set the user name and password programmatically or in the `server.xml` file.

A client can generate a UsernameToken with the user name and password provided in the `server.xml` file. The user name and password that is in the `server.xml` file is considered the default configuration and is overridden by what is provided on the `RequestContext` for the client's web service invocation.

The following example shows a sample default configuration:

```

<wsSecurityClient id="default"
  ws-security.username="alice"
  ws-security.callback-handler="com.acme.PasswordCallback"
</wsSecurityClient>

```

To generate a UsernameToken with the user name and password determined programmatically, you can set the following CXF properties on the `RequestContext` for the client's web service invocation:

- `ws-security.username` - user name
- `ws-security.password` - user password if `ws-security.callback-handler` is not defined
- `ws-security.callback-handler` - the `CallbackHandler` implementation class used to obtain passwords

The following code sample shows how to provide a user name and password on the request context:

```
Map<String, Object> requestCtx = ((BindingProvider)port).getRequestContext();
requestCtx.put("ws-security.username", "bob_username");
requestCtx.put("ws-security.password", "bob_password");
```

## Consuming a UsernameToken in a web services provider

When a `UsernameToken` is received, WS-Security automatically uses Liberty security user registry to validate the user name and password, if the password is required. If the password type in the `UsernameToken` is `PasswordDigest` or is using derived keys, you must provide the `ws-security.callback-handler` implementation of a password callback handler by configuring it in the `server.xml` file. This callback handler must return valid passwords for all expected user names so that the WS-Security run time can calculate digest values for comparison with the value in the SOAP message. After the digest value comparison completes successfully, the user name and password is validated against the user registry.

The following example illustrates a sample configuration in the `server.xml` file for password digest:

```
<wsSecurityProvider id="default"
  ws-security.callback-handler="com.acme.PasswordCallback"
</wsSecurityProvider>
```

## Password CallbackHandler

The password `CallbackHandler` is used by WS-Security to retrieve a user password. In Liberty, this password `CallbackHandler` class must be packaged as a Liberty feature. For more information about the password `CallbackHandler`, see [Developing a password callback handler for WS-Security](#).

For more information on requirements and limitations of a callback handler implementation, refer to the [Private key password CallbackHandler](#) section of [Protection of web services with an X.509 token](#).

## Protecting a UsernameToken in a SOAP message

When a `UsernameToken` is specified in a policy, the password type is password text (`PasswordText`) by default. When a password is sent with password text, it is sent in the message as-is. The following example shows a `UsernameToken` with a password type of `PasswordText`:

```
<UsernameToken>
  <Username>myusername</Username>
  <Password
    Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText">
    mypassword
  </Password>
</UsernameToken>
```

When you want to send a `UsernameToken` with `PasswordText`, you should consider additional protections on the message, such as using HTTPS or encrypting the token using the `EncryptedSupportingToken` policy assertion. For more information on requiring the use of the HTTPS transport in the policy, see [Liberty Profile: Web services security HTTPS transport policy assertions](#).

## UsernameToken key derivation

As stated in the [Web Services Security UsernameToken Profile 1.1](#) specification:

*The password associated with a username may be used to derive a shared secret key for the purposes of integrity or confidentiality protecting message contents.*

*It must be noted that passwords are subject to several kinds of attack, which in turn will lead to the exposure of any derived keys. This key derivation procedure is intended to minimize the risk of attacks on the keys, to the extent possible, but it is ultimately limited by the insecurity of a password that it is possible for a human being to remember and type on a standard keyboard.*

*Two additional elements are required to enable to derivation of a key from a password. They are <wsse11:Salt> and <wsse11:Iteration>. These values are not secret and must be conveyed in the Username token when key derivation is used. When key derivation is used the password must not be included in the Username token. The receiver will use its knowledge of the password to derive the same key as the sender.*

If a UsernameToken is using key derivation, for a provider application, you must provide the `ws-security.callback-handler` implementation of a password callback handler by configuring it in the `server.xml` file.

The following example shows a policy fragment for a UsernameToken as a protection token with key derivation:

```
<sp:SymmetricBinding>
  <wsp:Policy>
    <sp:ProtectionToken>
      <wsp:Policy>
        <sp:UsernameToken
          sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
          <wsp:Policy>
            <sp:WssUsernameToken10 />
            <sp:RequireDerivedKeys />
          </wsp:Policy>
        </sp:UsernameToken>
      </wsp:Policy>
    </sp:ProtectionToken>
  </wsp:Policy>
</sp:SymmetricBinding>
```

The following example shows a sample UsernameToken in the security header when key derivation is used:

```
<wsse:UsernameToken wsse:Id="...">
  <wsse:Username>...</wsse:Username>
  <wsse11:Salt>...</wsse11:Salt>
  <wsse11:Iteration>...</wsse11:Iteration>
</wsse:UsernameToken>
```

## Protection of web services with an X.509 token

### 8.5.5.0

Liberty supports the Oasis Web Services Security X.509 Certificate Token Profile 1.1. An X.509 token can be used to provide message integrity and confidentiality by signing and encrypting messages.

### WS-Security policy

To protect an XML message with an X.509 token, a contract that is specified in a Web Services Description Language (WSDL) must be created first. The web service must have a WS-Security policy included in the WSDL file. The WS-Security policy can contain `AsymmetricBinding` or `SymmetricBinding` assertions.

The requirement of an X.509 token is expressed as an `X509Token` assertion type in the WS-Security policy. The following example shows a sample `X509Token` assertion:

```

<sp:X509Token sp:IncludeToken=
  "http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
  <wsp:Policy>
    <sp:WssX509V3Token10 />
  </wsp:Policy>
</sp:X509Token>

```

In an AsymmetricBinding assertion:

- The initiator X509Token is used for message signature from the requestor to the provider and message encryption from the provider to the requestor.
- The recipient X509Token is used for message signature from the provider to the requestor and message encryption from the requestor to the provider.

The following table shows how the initiator and recipient tokens are used for each part of the request/response chain:

*Table 144. Initiator and recipient token use for each part of the request/response chain*

*	Initiator token	Recipient token
request out (requestor)	sign	encrypt
request in (provider)	verify signature	decrypt
response out (provider)	encrypt	sign
response in (requestor)	decrypt	verify signature

Private keys are used to sign and decrypt messages. Public certificates are used to encrypt messages and verify signatures. Private keys belong to the user of the key (the signer or decrypter).

In a SymmetricBinding assertion, a secret key or ephemeral key that is protected for an X.509 token is shared by both the initiator and the recipient, and the key is used for both encryption and decryption.

The following example shows a sample WS-Security policy with an X.509 token in an AsymmetricBinding assertion. This policy enables signing and encryption of the body for both the request and response with Timestamp.

```

<wsp:Policy wsu:Id="SampleAsymmetricX509TokensPolicy">
  <wsp:ExactlyOne>
    <wsp>All>
      <sp:AsymmetricBinding>
        <wsp:Policy>
          <sp:InitiatorToken>
            <wsp:Policy>
              <sp:X509Token sp:IncludeToken=
                "http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                <wsp:Policy>
                  <sp:WssX509V3Token10 />
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:InitiatorToken>
          <sp:RecipientToken>
            <wsp:Policy>
              <sp:X509Token sp:IncludeToken=
                "http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/Never">
                <wsp:Policy>
                  <sp:WssX509V3Token10 />
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:RecipientToken>
          <sp:AlgorithmSuite>
            <wsp:Policy>
              <sp:Basic128 />
            </wsp:Policy>
          </sp:AlgorithmSuite>
          <sp:Layout>
            <wsp:Policy>
              <sp:Strict />
            </wsp:Policy>
          </sp:Layout>
          <sp:IncludeTimestamp />
          <sp:ProtectTokens />
          <sp:OnlySignEntireHeadersAndBody />
        </wsp:Policy>
      </wsp>All>
    </wsp:ExactlyOne>
  </wsp:Policy>

```

```

    </wsp:Policy>
  </sp:AsymmetricBinding>
<sp:SignedParts>
  <sp:Body />
</sp:SignedParts>
<sp:EncryptedParts>
  <sp:Body />
</sp:EncryptedParts>
<sp:Wss10>
  <wsp:Policy>
    <sp:MustSupportRefKeyIdentifier />
  </wsp:Policy>
</sp:Wss10>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>

```

The following example shows a sample WS-Security policy with an X.509 token in a SymmetricBinding assertion. This policy enables signing of the Body for both the request and response with Timestamp.

```

<wsp:Policy wsu:Id="SampleSymmetricX509TokensPolicy">
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:SymmetricBinding>
        <wsp:Policy>
          <sp:ProtectionToken>
            <wsp:Policy>
              <sp:X509Token sp:IncludeToken=
                "http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/Never">
                <wsp:Policy>
                  <sp:WssX509V3Token11 />
                  <sp:RequireThumbprintReference />
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:ProtectionToken>
          <sp:Layout>
            <wsp:Policy>
              <sp:Lax />
            </wsp:Policy>
          </sp:Layout>
          <sp:IncludeTimestamp />
          <sp:OnlySignEntireHeadersAndBody />
          <sp:SignBeforeEncrypting />
          <sp:AlgorithmSuite>
            <wsp:Policy>
              <sp:Basic128 />
            </wsp:Policy>
          </sp:AlgorithmSuite>
        </wsp:Policy>
      </sp:SymmetricBinding>
      <sp:EncryptedParts>
        <sp:Body />
      </sp:EncryptedParts>
      <sp:SignedParts>
        <sp:Body />
      </sp:SignedParts>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>

```

## Token reference and token inclusion

A token assertion can carry an `sp:IncludeToken` attribute that requires that the token be included in the message. Several token assertions support mechanisms for referencing tokens in addition to direct references. If a token assertion contains multiple reference assertions, then the references to that token are required to contain all the specified reference types. For example, if a token assertion carries an `sp:IncludeToken` attribute with a value of `../Always` and that token assertion also contains a nested `sp:RequireIssuerSerialReference` assertion, then the token must be included twice in the message. While such combinations are not errors, they are best avoided for efficiency reasons.

The `IncludeToken` assertion is enforced in Liberty, but is ignored in the WS-Security runtime environment of WebSphere Application Server traditional.

The WS-Security policy supports the following token reference mechanisms:

- `KeyIdentifier`: `<sp:RequireKeyIdentifierReference... />`
- `IssuerSerial`: `<sp:RequireIssuerSerialReference ... />`

- Thumbprint: <sp:RequireThumbprintReference ... />

These references are used when generating an X.509 token on the client/generator side, and are not enforced on the server/consumer side.

## Runtime configuration

The WS-Security feature run time in Liberty provides more configuration options for message protection with an X.509 token than are covered by the WS-Security policy. The runtime configuration is defined in the server.xml file. The runtime configuration includes cryptographic properties such as signatureProperties and encryptionProperties, key, and keystores.

The following example shows a client configuration for an X509Token assertion:

```
<wsSecurityClient id="default"
  ws-security.callback-handler="com.ibm.ws.wssecurity.example.cbh.KeyPasswordCallbackHandler">
  <signatureProperties org.apache.ws.security.crypto.merlin.keystore.type="jks"
    org.apache.ws.security.crypto.merlin.keystore.password="LibertyX509Client"
    org.apache.ws.security.crypto.merlin.keystore.alias="x509ClientDefault"
    org.apache.ws.security.crypto.merlin.file="{server.config.dir}/x509ClientDefault.jks" />
  <encryptionProperties org.apache.ws.security.crypto.merlin.keystore.type="jks"
    org.apache.ws.security.crypto.merlin.keystore.password="LibertyXClient"
    org.apache.ws.security.crypto.merlin.keystore.alias="x509DefaultCert"
    org.apache.ws.security.crypto.merlin.file="{server.config.dir}/x509ClientDefault.jks" />
</wsSecurityClient>
```

The following example shows a server configuration for an X509Token assertion:

```
<wsSecurityProvider id="default"
  ws-security.callback-handler="com.ibm.ws.wssecurity.example.cbh.KeyPasswordCallbackHandler">
  <signatureProperties org.apache.ws.security.crypto.merlin.keystore.type="jks"
    org.apache.ws.security.crypto.merlin.keystore.password="LibertyX509Server"
    org.apache.ws.security.crypto.merlin.keystore.alias="x509ServerDefault"
    org.apache.ws.security.crypto.merlin.file="{server.config.dir}/x509ServerDefault.jks" />
  <encryptionProperties org.apache.ws.security.crypto.merlin.keystore.type="jks"
    org.apache.ws.security.crypto.merlin.keystore.password="LibertyX509Server"
    org.apache.ws.security.crypto.merlin.keystore.alias="x509ServerDefault"
    org.apache.ws.security.crypto.merlin.file="{server.config.dir}/x509ServerDefault.jks" />
</wsSecurityProvider>
```

In the runtime configuration, the signatureProperties and encryptionProperties properties are equivalent to the crypto properties in the WSS4J configuration. See WSS4J configuration for additional details. Many crypto properties have valid default values so there is no need to specify them. But other properties, such as keystore and key related properties, must be specified.

For more information about these properties, see Web services security default configuration.

## Keystore files, keys, and certificates

Message signature and encryption requires the use of public certificates and private keys. These public certificates and private keys are stored in keystore files. Keystore files are required when you use X509Token assertions. The client-side keystore file contains the private key of the client, and a chain of certificates corresponding to the public key of the server. The server-side keystore file contains the private key of the server, and a chain of certificates corresponding to the public key of the client.

When a SOAP message is signed and encrypted, the signatureProperties and encryptionProperties properties are interpreted by the WS-Security runtime environment as follows:

- AsymmetricBinding assertion

The key specified by the signatureProperties property is used as the private key for signing the outbound message, and is also used for decrypting the inbound message.

The key specified by the encryptionProperties property is used as the public key for encrypting the outbound message, and is also used for verifying the signature in the inbound message.

- SymmetricBinding assertion

The key specified by the `encryptionProperties` properties is used, while the `signatureProperties` property is ignored.

## Private key password CallbackHandler

To access a private key in a keystore, you must know two different passwords. One password is for the keystore where the private key is stored. The other password is for the private key itself. While the password for the keystore is specified in one of the crypto properties, either `signatureProperties` or `encryptionProperties`, the `CallbackHandler` class is normally used by WS-Security to access the private key in a keystore. In Liberty, this `CallbackHandler` class must be packaged as a Liberty feature and its class name specified as the value for the `ws-security.callback-handler` custom property in the `security.xml`.

This `CallbackHandler` class is required by WS-Security to access the private key in a keystore.

For more information about the password `CallbackHandler` class, see [Developing a password callback handler for WS-Security](#).

If the `CallbackHandler` class does not provide the private key password, the `ws-security` runtime first tries the `CallbackHandler` so it must be provided, then the password that is specified in the crypto properties is used as the default password for the private key. This property is configured as `org.apache.ws.security.crypto.merlin.keystore.private.password`.

Because there is only one `ws-security.callback-handler` custom property supported in each of the `wsSecurityClient` and `wsSecurityProvider` sections of the `security.xml` file, a single password callback handler must support all of the required passwords for each application type (client or server) that use the default. All provider applications must use the default password callback handler. Client applications can override the default callback handler by specifying the `ws-security.callback-handler` custom property on the request context for the web service invocation of the client.

If you need to provide passwords for an X.509 private key and a `UsernameToken` for a single web service invocation, you cannot provide separate callback handlers for each use. In this case, you must implement a single callback handler that handles both kinds of passwords. As illustrated in the previous example, you must use the `WSPasswordCallback.getUsage()` method to determine which kind of password that you should return. See the `WSPasswordCallback` API documentation for the supported usage codes: <http://ws.apache.org/wss4j/apidocs/org/apache/wss4j/common/ext/WSPasswordCallback.html>.

### 8.5.5.0

## Certificate revocation list

A certificate revocation list (CRL) is a list of serial numbers for certificates that have been revoked. A CRL can be a stand-alone file or it can be packaged in a PKCS#7 wrapper. You can use a CRL in conjunction with a trust store to control access to a service.

There are two steps required to configure the WS-Security feature in Liberty to perform revocation checking with a CRL file. To enable certificate revocation checking with a CRL file, you must modify the WS-Security runtime configuration in the `server.xml` file.

1. Within the `wsSecurityProvider` or `wsSecurityClient` element, add the following property:  
`ws-security.enableRevocation="true"`
2. Within the `signatureProperties` element, add the following property and set the value to a CRL file:  
`org.apache.ws.security.crypto.merlin.x509crl.file`

The following example shows a sample WS-Security provider configuration that enables certificate revocation checking with a CRL file:

```

<wsSecurityProvider id="default"
  ws-security.callback-handler="com.acme.example.cbh.CommonPasswordCallback"
  ws-security.signature.username="x509ServerDefault"
  ws-security.enableRevocation="true">
  <signatureProperties
    org.apache.ws.security.crypto.merlin.keystore.type="jks"
    org.apache.ws.security.crypto.merlin.keystore.password="LibertyX509Server"
    org.apache.ws.security.crypto.merlin.keystore.alias="x509ServerDefault"
    org.apache.ws.security.crypto.merlin.file="${server.config.dir}/x509ServerDefault.ks"
    org.apache.ws.security.crypto.merlin.truststore.password="LibertyX509Server"
    org.apache.ws.security.crypto.merlin.truststore.file="${server.config.dir}/x509DefaultServer.ks"
    org.apache.ws.security.crypto.merlin.x509crl.file="${server.config.dir}/revokedCerts.crl"/>
</wsSecurityProvider>

```

## Protection of web services with endorsing tokens

**8.5.6.0**

An endorsing token is used to sign the SOAP message signature. An endorsing token is usually used to sign the entire <Signature> element and optionally to sign additional message parts. If transport security is used, the endorsing token must be used to sign the Timestamp in the SOAP Security header.

### Endorsing supporting token assertions

Endorsing tokens are SupportingTokens in WS-Security, and can be signed and encrypted. There are four types of endorsing tokens.

- EndorsingSupportingTokens - The token is not required to be signed or encrypted.
- SignedEndorsingSupportingTokens - The token must be signed.
- EndorsingEncryptedSupportingTokens - The token must be encrypted.
- SignedEndorsingEncryptedSupportingTokens - The token must be signed.

### X509Token as an endorsing token

You can configure an X509Token as an endorsing token. Configuring an X509Token as an endorsing token is similar to configuring an X509Token as an InitiatorToken in an AsymmetricBinding. To configure an X509Token as an endorsing token, you need a policy that has an X509Token contained within one of the endorsing token assertions described previously, and a <SignatureProperties> element in the server.xml file.

The following example shows a policy fragment for an X509 endorsing supporting token:

```

<sp:EndorsingSupportingTokens xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
  <wsp:Policy>
    <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
      <wsp:Policy>
        <sp:WssX509V3Token10/>
      </wsp:Policy>
    </sp:X509Token>
  </wsp:Policy>
</sp:EndorsingSupportingTokens>

```

After configuring the X509Token as an endorsing token, you must define the <signatureProperties> element in the server.xml file to identify the keystore and the signing key. The configuration for the <signatureProperties> element is the same as the configuration of the X509Token for the message signature. For more information, see Protection of web services with an X.509 token.

### UsernameToken as an endorsing token

The configuration of a UsernameToken as an endorsingToken is similar to the configuration of a UsernameToken with PasswordDigest, except there is no HashPassword in the policy. To configure a

UsernameToken as an endorsing token, you need a policy that has a UsernameToken contained within one of the endorsing token assertions described in the Endorsing supporting token assertions section.

The following example shows a policy fragment for a UsernameToken signed and encrypted endorsing supporting token. Key derivation is used:

```
<sp:SignedEndorsingEncryptedSupportingTokens>
  <wsp:Policy>
    <sp:UsernameToken
      sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
      <wsp:Policy>
        <sp:WssUsernameToken10 />
        <sp:RequireDerivedKeys />
      </wsp:Policy>
    </sp:UsernameToken>
  </wsp:Policy>
</sp:SignedEndorsingEncryptedSupportingTokens>
```

In this sample policy fragment, the UsernameToken is signed and encrypted with the rest of the message. Then the key that is derived from the password from the UsernameToken is used to sign the message signature.

Since a UsernameToken endorsing token uses derived keys, you must implement and configure a password CallbackHandler for a provider application. For more information, see Authentication of web services clients with a UsernameToken.

## Web services security caller configuration

### 8.5.5.0

You can run a web service in authenticated or unauthenticated mode. When you want to restrict access to resources based on the identity of a user, the web service must run in authenticated mode. When a web service is run in authenticated mode, the identity of the user is placed on the same thread on which the web service runs.

There are two ways that a web service can run in the authenticated mode:

#### HTTP basic authentication

The identity from the HTTP header is placed on the thread by the web container.

#### WS-Security caller configuration

The identity of one of the tokens in the SOAP security header is placed on the thread by the WS-Security runtime.

The WS-Security specification allows more than one token to be passed in the security header of a SOAP message. When a web service is required to run in authenticated mode by using WS-Security, some mechanism is required to tell the WS-Security runtime environment which token to use for the identity. This mechanism is called a caller configuration.

The WS-Security caller configuration is specified in the `server.xml` file with the `<callerToken>` element.

The following example shows a sample WS-Security provider configuration that includes a caller configuration for a UsernameToken:

```
<wsSecurityProvider ...>
  ...
  <callerToken name="UsernameToken" />
  ...
</wsSecurityProvider>
```

The following values can be specified for the `<callerToken>` element:

- UsernameToken

- X509Token
- **8.5.5.8** SamlToken

If you configure an X509Token as a caller token, make sure only one client's X509Certificate can be resolved from the security header. For example, ensure that only one client certificate is resolved from the initiator token in an AsymmetricBinding, or that only one client certificate that is resolved from an endorsing token.

If you configure a UsernameToken as a caller token, the security header must contain only one UsernameToken.

**8.5.5.8** If you configure a SamlToken as a caller token, the security header must contain only one SAML token. There are additional configuration options such as `userIdentifier`, `groupIdentifier` or `realmIdentifier` that is used to specify a SAML attribute that can be used as a principal, group or realm when an authenticated subject is created. For more information about the optional SAML callerToken configuration, see "Creating a WS-Security SAML caller configuration."

### Creating a WS-Security SAML caller configuration: **8.5.5.8**

A WS-Security provider configuration that includes a caller for a SAML token can be configured with the `<callerToken>` element in the `server.xml` file.

#### Procedure

1. Configure the WS-Security Security Assertion Markup Language (SAML) caller configuration in the `server.xml` file with the `<callerToken>` element. The following example shows a sample WS-Security provider configuration that includes a caller for a SAML Token:

```
<wsSecurityProvider ...>
  ...
  <callerToken name="SamlToken" userIdentifier="userIdentifierString" groupIdentifier="groupIdentifierString" userUniqueIdentifier="userUniqueIdentifierString"
    includeTokenInSubject="false" mapToUserRegistry="User" realmName="customRealmName" allowCustomCacheKey="true" ... />
  ...
</wsSecurityProvider>
```

The only required attribute in this configuration is `name`. By default, the authenticated subject is created by using the information from the SAML assertion and it does not require a local user registry to do the authentication.

2. Optional: You can configure the following optional attributes to help create an authenticated subject from SAML assertion. The default values for some of these optional attributes are:

```
includeTokenInSubject=true
mapToUserRegistry="No"
allowCustomCacheKey="true"
```

- When `mapToUserRegistry` is `"No"`, the name of the SAML issuer is used as realm, and the `NameID` is used as the principal name and unique security name in the subject, and the group member is not included.
- When `mapToUserRegistry` is `"User"`, the SAML user is validated against your on-premises user registry, and then the runtime creates the user subject based on the on-premises registry.
- When `mapToUserRegistry` is `"Group"`, SAML group is validated against your on-premises user registry, and then the runtime creates the subject with the validated groups. This option is similar to `mapToUserRegistry=No`, except for the verification of the group memberships against the on-premises user registry.

You can configure additional attributes such as `userIdentifier`, `realmIdentifier`, `groupIdentifier`, and `userUniqueIdentifier` to create an authenticated subject with a customized user name, realm name, group memberships, and unique security identifier.

- `userIdentifier`: Use this attribute to select a SAML attribute name whose value is used as the principal name.

- `groupId`: Use this attribute to select a SAML attribute name whose values are included as group members in the subject.
  - `realmName`: Use this attribute to explicitly specify the realm name to identify a SAML principal for the authenticated subject. The default realm name is the SAML issuer name.
3. Optional: You can implement the Liberty SAML SPI, `com.ibm.wsspi.security.saml2.UserCredentialResolver` as a user feature to dynamically map a SAML assertion to a Liberty subject.

## WS-SecurityPolicy and templates

### 8.5.5.0

Web Services Security (WS-Security) in Liberty is configured by using the WS-SecurityPolicy in either Web Services Description Language (WSDL) or policy attachment file of a web service application. To protect your web service application with WS-Security, your JAX-WS application must contain a WSDL or policy attachment file that has an embedded WS-Security Policy. WS-SecurityPolicy templates contain several commonly used WS-Security policy samples. These templates can be modified to satisfy many different usage scenarios.

The following list of commonly used WS-SecurityPolicy templates are provided, and can be modified to satisfy many different usage scenarios:

- Scenario 1: UsernameToken with password digest (HashPassword) and timestamp over SSL
- Scenario 2: UsernameToken with password text, nonce, and created timestamp over SSL
- Scenario 3: UsernameToken as an EndorsingToken and an X509Token symmetric for message protection
- Scenario 4: UsernameToken with X509Token asymmetric message protection (mutual authentication)
- Scenario 5: Client X509Token as an EndorsingToken and a server X509Token symmetric for message protection
- Scenario 6: UsernameToken authentication and an X509Token symmetric for message protection
- Scenario 7: UsernameToken with password text, nonce, and created timestamp over HTTP
- **8.5.5.8** Scenario 8: SAMLToken as SupportingToken over SSL
- **8.5.5.8** Scenario 9: SAMLToken with X509Token asymmetric for message signature
- **8.5.5.8** Scenario 10: SAMLToken with X509Token asymmetric message protection (mutual authentication)
- **8.5.5.8** Scenario 11: SAMLToken with X509Token symmetric for message protection

### UsernameToken with password digest (HashPassword) and timestamp over SSL: **8.5.5.0**

This policy requires that you protect the message with HTTPS, and that a UsernameToken is used for authentication. The UsernameToken password is hashed with the created timestamp and nonce. There is also a message Timestamp.

The following policy shows a UsernameToken with password digest (HashPassword) and timestamp over SSL:

```
<wsp:Policy wsu:Id="UserNameTokenPasswordHashOverSSL">
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:TransportBinding>
        <wsp:Policy>
          <sp:TransportToken>
            <wsp:Policy>
              <sp:HttpsToken>
                <wsp:Policy />
              </sp:HttpsToken>
            </wsp:Policy>
          </sp:TransportToken>
        </wsp:Policy>
      </sp:Layout>
    </wsp:Policy>
  </wsp:ExactlyOne>
</wsp:Policy>
```

```

        <sp:Lax />
    </wsp:Policy>
</sp:Layout>
<sp:IncludeTimestamp />
<sp:AlgorithmSuite>
    <wsp:Policy>
        <sp:Basic128 />
    </wsp:Policy>
</sp:AlgorithmSuite>
</wsp:Policy>
</sp:TransportBinding>
<sp:SupportingTokens>
    <wsp:Policy>
        <sp:UsernameToken
            sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
            <wsp:Policy>
                <sp:WssUsernameToken10 />
                <sp:HashPassword/>
            </wsp:Policy>
        </sp:UsernameToken>
    </wsp:Policy>
</sp:SupportingTokens>
</wsp>All>
</wsp:ExactlyOne>
</wsp:Policy>

```

The namespaces used in this example are:

- xmlns:wsp="http://www.w3.org/ns/ws-policy"
- xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
- xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"

To validate the UsernameToken in the Liberty profile server, you must provide a password callback handler class on the provider side by setting the ws-security.callback-handler attribute. The password from the callback handler must match the password that is used in the PasswordDigest. The password must also match the password in the user registry in the Liberty profile.

### UsernameToken with password text, nonce, and created timestamp over SSL: **8.5.5.0**

This policy requires that you protect the message with HTTPS, and that a UsernameToken is used for authentication. The user password within the UsernameToken is sent as clear text, and a timestamp and nonce are included. There is also a message Timestamp. You can modify this policy to remove the requirement of nonce and timestamp. For testing purposes, you can also remove the TransportBinding to send the UsernameToken over HTTP for simplicity.

The following policy shows a UsernameToken with password text, nonce, and created timestamp over SSL:

```

<wsp:Policy wsu:Id="UserNameTokenPasswordTextOverSSL">
    <wsp:ExactlyOne>
        <wsp>All>
            <sp:TransportBinding>
                <wsp:Policy>
                    <sp:TransportToken>
                        <wsp:Policy>
                            <sp:HttpsToken>
                                <wsp:Policy>
                                    </wsp:Policy>
                                </sp:HttpsToken>
                            </wsp:Policy>
                        </sp:TransportToken>
                    </wsp:Policy>
                </sp:Layout>
                <wsp:Policy>
                    <sp:Lax />
                </wsp:Policy>
            </sp:Layout>
            <sp:IncludeTimestamp />
            <sp:AlgorithmSuite>
                <wsp:Policy>

```

```

        <sp:Basic128 />
    </wsp:Policy>
</sp:AlgorithmSuite>
</wsp:Policy>
</sp:TransportBinding>
<sp:SupportingTokens>
  <wsp:Policy>
    <sp:UsernameToken
      sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
      <wsp:Policy>
        <sp:WssUsernameToken10 />
        <sp13:Created />
        <sp13:Nonce />
      </wsp:Policy>
    </sp:UsernameToken>
  </wsp:Policy>
</sp:SupportingTokens>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>

```

The namespaces used in this example are:

- xmlns:wsp="http://www.w3.org/ns/ws-policy"
- xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
- xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"

This policy is analogous to the Username WSHTTPS default policy set in WebSphere Application Server traditional.

#### UsernameToken as an EndorsingToken and an X509Token symmetric for message protection:

##### 8.5.5.0

With X509Token symmetric protection, an ephemeral key is created to sign and encrypt the message. The ephemeral key is encrypted using the receiver's public certificate. A UsernameToken with derived keys is used for authentication. The message signature is signed using the UsernameToken's derived key. There is also a message Timestamp.

This policy template can be used if HTTP transport is not supported, the service has an X509 token and supports a UsernameToken, and the service requires the client to endorse the message.

The following policy shows a UsernameToken as an EndorsingToken and an X509Token symmetric for message protection:

```

<wsp:Policy wsu:Id="UsernameTokenAsEndorsingAndX509Symmetric">
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:SymmetricBinding>
        <wsp:Policy>
          <sp:ProtectionToken>
            <wsp:Policy>
              <sp:X509Token
                sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                <wsp:Policy>
                  <sp:WssX509V3Token10 />
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:ProtectionToken>
          <sp:Layout>
            <wsp:Policy>
              <sp:Lax />
            </wsp:Policy>
          </sp:Layout>
          <sp:IncludeTimestamp />
          <sp:OnlySignEntireHeadersAndBody />
          <sp:AlgorithmSuite>
            <wsp:Policy>

```

```

        <sp:Basic128 />
    </wsp:Policy>
</sp:AlgorithmSuite>
</wsp:Policy>
</sp:SymmetricBinding>
<sp:SignedEndorsingEncryptedSupportingTokens>
    <wsp:Policy>
        <sp:UsernameToken
            sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
            <wsp:Policy>
                <sp:WssUsernameToken10 />
                <sp:RequireDerivedKeys />
            </wsp:Policy>
        </sp:UsernameToken>
    </wsp:Policy>
</sp:SignedEndorsingEncryptedSupportingTokens>
<sp:SignedParts>
    <sp:Body />
</sp:SignedParts>
<sp:EncryptedParts>
    <sp:Body />
</sp:EncryptedParts>
</wsp>All>
</wsp:ExactlyOne>
</wsp:Policy>

```

The namespaces used in this example are:

- xmlns:wsp="http://www.w3.org/ns/ws-policy"
- xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
- xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"

### UsernameToken with X509Token asymmetric message protection (mutual authentication):

**8.5.5.0**

An X509Token with issuer/serial representation of the sender's public certificate is included in the message. The UsernameToken in the request and the SOAP body in the request and response are signed and encrypted with X509Token asymmetric message protection. There is also a message Timestamp and signature confirmation. A UsernameToken with clear text password is used for authentication.

This policy template is best used if the client must authenticate itself to the service with both an X509 client certificate and a UsernameToken.

The following policy shows a UsernameToken with X509Token asymmetric message protection:

```

<wsp:Policy wsu:Id="AsymmetricX509MutualAuthenticationWithUnt">
    <wsp:ExactlyOne>
        <wsp>All>
            <sp:SignedEncryptedSupportingTokens
                xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
                <wsp:Policy>
                    <sp:UsernameToken
                        sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                        <wsp:Policy>
                            <sp:WssUsernameToken10 />
                        </wsp:Policy>
                    </sp:UsernameToken>
                </wsp:Policy>
            </sp:SignedEncryptedSupportingTokens>
            <sp:AsymmetricBinding>
                <wsp:Policy>
                    <sp:InitiatorToken>
                        <wsp:Policy>
                            <sp:X509Token
                                sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                                <wsp:Policy>
                                    <sp:WssX509V3Token10 />
                                    <sp:RequireIssuerSerialReference />
                                </wsp:Policy>
                            </sp:X509Token>

```

```

    </wsp:Policy>
  </sp:InitiatorToken>
  <sp:RecipientToken>
    <wsp:Policy>
      <sp:X509Token
        sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/Never">
        <wsp:Policy>
          <sp:WssX509V3Token10 />
          <sp:RequireIssuerSerialReference />
        </wsp:Policy>
      </sp:X509Token>
    </wsp:Policy>
  </sp:RecipientToken>
  <sp:Layout>
    <wsp:Policy>
      <sp:Strict />
    </wsp:Policy>
  </sp:Layout>
  <sp:IncludeTimestamp />
  <sp:OnlySignEntireHeadersAndBody />
  <sp:EncryptSignature />
  <sp:AlgorithmSuite>
    <wsp:Policy>
      <sp:Basic128 />
    </wsp:Policy>
  </sp:AlgorithmSuite>
</wsp:Policy>
</sp:AsymmetricBinding>
<sp:Wss11>
  <wsp:Policy>
    <sp:MustSupportRefKeyIdentifier />
    <sp:MustSupportRefIssuerSerial />
    <sp:MustSupportRefThumbprint />
    <sp:MustSupportRefEncryptedKey />
    <sp:RequireSignatureConfirmation />
  </wsp:Policy>
</sp:Wss11>
<sp:SignedParts>
  <sp:Body />
</sp:SignedParts>
<sp:EncryptedParts>
  <sp:Body />
</sp:EncryptedParts>
</wsp>All>
</wsp:ExactlyOne>
</wsp:Policy>

```

The namespaces used in this example are:

- xmlns:wsp="http://www.w3.org/ns/ws-policy"
- xmlns:wssu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
- xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"

This policy is analogous to the Username WSSecurity default policy set in WebSphere Application Server traditional.

#### Client X509Token as an EndorsingToken and a server X509Token symmetric for message protection:

##### 8.5.5.0

The client and server X509 certificates are used for mutual authentication and message protection. With X509Token symmetric protection, an ephemeral key is created to sign and encrypt the message. The ephemeral key is encrypted using the receiver's public certificate. An X509Token with the thumbprint representation of the client's public certificate is included in the message. The message signature is signed using the client's private key.

This policy template is best used if the client must authenticate itself to the service with both an X509 client certificate and a UsernameToken.

The following policy shows a client X509Token as an EndorsingToken and a server X509Token symmetric for message protection:

```
<wsp:Policy wsu:Id="X509SymmetricAndEndorsing">
  <wsp:ExactlyOne>
    <wsp>All>
      <sp:SymmetricBinding>
        <wsp:Policy>
          <sp:ProtectionToken>
            <wsp:Policy>
              <sp:X509Token
                sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/Never">
                <wsp:Policy>
                  <sp:RequireDerivedKeys />
                  <sp:RequireThumbprintReference />
                  <sp:WssX509V3Token11 />
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:ProtectionToken>
          <sp:AlgorithmSuite>
            <wsp:Policy>
              <sp:Basic128 />
            </wsp:Policy>
          </sp:AlgorithmSuite>
          <sp:Layout>
            <wsp:Policy>
              <sp:Strict />
            </wsp:Policy>
          </sp:Layout>
          <sp:IncludeTimestamp />
          <sp:OnlySignEntireHeadersAndBody />
        </wsp:Policy>
      </sp:SymmetricBinding>
      <sp:EncryptedParts>
        <sp:Body />
      </sp:EncryptedParts>
      <sp:SignedParts>
        <sp:Body />
      </sp:SignedParts>
      <sp:EndorsingSupportingTokens xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <wsp:Policy>
          <sp:X509Token
            sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
            <wsp:Policy>
              <sp:RequireThumbprintReference />
              <sp:WssX509V3Token11 />
            </wsp:Policy>
          </sp:X509Token>
        </wsp:Policy>
      </sp:EndorsingSupportingTokens>
      <sp:Wss11>
        <wsp:Policy>
          <sp:MustSupportRefKeyIdentifier />
          <sp:MustSupportRefIssuerSerial />
          <sp:MustSupportRefThumbprint />
          <sp:MustSupportRefEncryptedKey />
          <sp:RequireSignatureConfirmation />
        </wsp:Policy>
      </sp:Wss11>
    </wsp>All>
  </wsp:ExactlyOne>
</wsp:Policy>
```

The namespaces used in this example are:

- xmlns:wsp="http://www.w3.org/ns/ws-policy"
- xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
- xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"

## UsernameToken authentication and X509Token symmetric for message protection: 8.5.5.0

A UsernameToken with clear text password is used for authentication. The UsernameToken in the request and the SOAP body in the request and response are signed and encrypted with X509Token symmetric message protection. There is also a message Timestamp.

With X509Token symmetric protection, an ephemeral key is created to sign and encrypt the message. The ephemeral key is encrypted using the receiver's public certificate.

In this sample, the token reference is using a RequireThumbprintReference. You can change the policy to use a RequireIssuerSerialReference or RequireKeyIdentifierReference. You can also modify this policy to use derived keys from an ephemeral key to secure the message exchange by adding an `<sp:RequireDerivedKeys />` assertion.

This policy template is best used if the client can use only a UsernameToken to authenticate itself, and if the message exchange must be signed and encrypted.

The following policy shows a UsernameToken authentication and X509Token symmetric for message protection:

```
<wsp:Policy wsu:Id="X509SymmetricForMessageAndUntForClient">
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:SignedEncryptedSupportingTokens
        xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <wsp:Policy>
          <sp:UsernameToken
            sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
            <wsp:Policy>
              <sp:WssUsernameToken10 />
            </wsp:Policy>
          </sp:UsernameToken>
        </wsp:Policy>
      </sp:SignedEncryptedSupportingTokens>
      <sp:SymmetricBinding>
        <wsp:Policy>
          <sp:ProtectionToken>
            <wsp:Policy>
              <sp:X509Token
                sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/Never">
                <wsp:Policy>
                  <sp:RequireThumbprintReference />
                  <sp:WssX509V3Token10 />
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:ProtectionToken>
          <sp:AlgorithmSuite>
            <wsp:Policy>
              <sp:Basic128 />
            </wsp:Policy>
          </sp:AlgorithmSuite>
          <sp:Layout>
            <wsp:Policy>
              <sp:Strict />
            </wsp:Policy>
          </sp:Layout>
          <sp:IncludeTimestamp />
          <sp:OnlySignEntireHeadersAndBody />
          <sp:EncryptSignature />
        </wsp:Policy>
      </sp:SymmetricBinding>
      <sp:Wss11>
        <wsp:Policy>
          <sp:MustSupportRefKeyIdentifier />
          <sp:MustSupportRefIssuerSerial />
          <sp:MustSupportRefThumbprint />
          <sp:MustSupportRefEncryptedKey />
          <sp:RequireSignatureConfirmation />
        </wsp:Policy>
      </sp:Wss11>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>
```

```

    <sp:SignedParts>
      <sp:Body />
    </sp:SignedParts>
    <sp:EncryptedParts>
      <sp:Body />
    </sp:EncryptedParts>
  </wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>

```

The namespaces used in this example are:

- xmlns:wsp="http://www.w3.org/ns/ws-policy"
- xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
- xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"

### UsernameToken with password text, nonce, and created timestamp over HTTP: 8.5.5.0

This policy requires that a client must send a UsernameToken with clear text password, nonce, and created timestamp. Transport security is not required. This simple policy is only suitable if password confidentiality is not a concern or is provided by other means. This policy can be used in a pre-production environment for testing purposes.

The following policy shows a UsernameToken with password text, nonce, and created timestamp over HTTP:

```

<wsp:Policy wsu:Id="UsernameTokenOverHTTP">
  <sp:SupportingTokens>
    <wsp:Policy>
      <sp:UsernameToken
        sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
        <wsp:Policy>
          <sp13:Created />
          <sp13:Nonce />
          <sp:WssUsernameToken11 />
        </wsp:Policy>
      </sp:UsernameToken>
    </wsp:Policy>
  </sp:SupportingTokens>
</wsp:Policy>

```

The namespaces used in this example are:

- xmlns:wsp="http://www.w3.org/ns/ws-policy"
- xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
- xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"

### Sam1Token as SupportingToken over SSL: 8.5.5.8

This policy requires that you protect the message with HTTPS, and that a SAML 2.0 token is used for authentication.

The following policy shows a SAML 2.0 token over SSL:

```

<wsp:Policy wsu:Id="Sam120TokenOverSSL">
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:TransportBinding>
        <wsp:Policy>
          <sp:TransportToken>
            <wsp:Policy>
              <sp:HttpsToken>
                <wsp:Policy/>
              </sp:HttpsToken>
            </wsp:Policy>
          </sp:TransportToken>
        </wsp:Policy>
      </sp:TransportBinding>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>

```

```

    </sp:TransportToken>
    <sp:Layout>
      <wsp:Policy>
        <sp:Lax />
      </wsp:Policy>
    </sp:Layout>
    <sp:IncludeTimestamp />
    <sp:AlgorithmSuite>
      <wsp:Policy>
        <sp:Basic128 />
      </wsp:Policy>
    </sp:AlgorithmSuite>
  </wsp:Policy>
</sp:TransportBinding>
<sp:SupportingTokens>
  <wsp:Policy>
    <sp:SamlToken
      sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
      <wsp:Policy>
        <sp:WssSamlV20Token11/>
      </wsp:Policy>
    </sp:SamlToken>
  </wsp:Policy>
</sp:SupportingTokens>
</wsp>All>
</wsp:ExactlyOne>
</wsp:Policy>

```

### SAMLToken with X509Token asymmetric for message signature: 8.5.5.6

An X509Token with the sender's public certificate is included in the message. The SAML token in the request and the SOAP body in the request and response are signed with X509Token asymmetric message protection. A Timestamp is also included in the message. A SAML 2.0 token is used for authentication.

The following policy shows a SAMLToken with X509Token asymmetric for message signature:

```

<wsp:Policy wsu:Id="SamlTokenWithMessageSignature">
  <wsp:ExactlyOne>
    <wsp>All>
      <sp:SignedSupportingTokens>
        <wsp:Policy>
          <sp:SamlToken
            sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
            <wsp:Policy>
              <sp:WssSamlV20Token11/>
            </wsp:Policy>
          </sp:SamlToken>
        </wsp:Policy>
      </sp:SignedSupportingTokens>
      <sp:AsymmetricBinding >
        <wsp:Policy>
          <sp:InitiatorToken>
            <wsp:Policy>
              <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                <wsp:Policy>
                  <sp:WssX509V3Token10/>
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:InitiatorToken>
          <sp:RecipientToken>
            <wsp:Policy>
              <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                <wsp:Policy>
                  <sp:WssX509V3Token10/>
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:RecipientToken>
          <sp:AlgorithmSuite>
            <wsp:Policy>
              <sp:Basic128/>
            </wsp:Policy>
          </sp:AlgorithmSuite>
        </wsp:Policy>
      </sp:AsymmetricBinding>
    </wsp>All>
  </wsp:ExactlyOne>
</wsp:Policy>

```

```

        <sp:Lax/>
    </wsp:Policy>
</sp:Layout>
<sp:IncludeTimestamp/>
<sp:OnlySignEntireHeadersAndBody/>
</wsp:Policy>
</sp:AsymmetricBinding>
<sp:Wss10>
    <wsp:Policy>
        <sp:MustSupportRefKeyIdentifier/>
    </wsp:Policy>
</sp:Wss10>
<sp:SignedParts>
    <sp:Body/>
</sp:SignedParts>
</wsp>All>
</wsp:ExactlyOne>
</wsp:Policy>

```

### SamlToken with X509Token asymmetric message protection (mutual authentication): 8.5.5.8

An X509Token with issuer and serial representation of the sender's public certificate is included in the message. The SAML token in the request and the SOAP body in the request and response are signed and encrypted with X509Token asymmetric message protection. There is also a message timestamp and signature confirmation. A SAML 2.0 token is used for authentication. This policy template is best used if the client must authenticate itself to the service with both an X509 client certificate and a SAML token.

The following policy shows a SAML token with X509Token asymmetric message protection:

```

<wsp:Policy wsu:Id="AsymmetricX509MutualAuthenticationWithSam1">
  <wsp:ExactlyOne>
    <wsp>All>
      <sp:SignedEncryptedSupportingTokens
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <wsp:Policy>
          <sp:Sam1Token
            sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <wsp:Policy>
                <sp:WssSam1V20Token11/>
              </wsp:Policy>
            </sp:Sam1Token>
          </wsp:Policy>
        </sp:SignedEncryptedSupportingTokens>
        <sp:AsymmetricBinding>
          <wsp:Policy>
            <sp:InitiatorToken>
              <wsp:Policy>
                <sp:X509Token
sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                  <wsp:Policy>
                    <sp:WssX509V3Token10 />
                    <sp:RequireIssuerSerialReference />
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:InitiatorToken>
            <sp:RecipientToken>
              <wsp:Policy>
                <sp:X509Token
sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:WssX509V3Token10 />
                    <sp:RequireIssuerSerialReference />
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:RecipientToken>
          </sp:Layout>
          <wsp:Policy>
            <sp:Strict />
          </wsp:Policy>
        </sp:Layout>
        <sp:IncludeTimestamp />
        <sp:OnlySignEntireHeadersAndBody />
        <sp:EncryptSignature />
      </wsp:Policy>
    </wsp>All>
  </wsp:ExactlyOne>
</wsp:Policy>

```

```

    <sp:AlgorithmSuite>
      <wsp:Policy>
        <sp:Basic128 />
      </wsp:Policy>
    </sp:AlgorithmSuite>
  </wsp:Policy>
</sp:AsymmetricBinding>
<sp:Wss11>
  <wsp:Policy>
    <sp:MustSupportRefKeyIdentifier />
    <sp:MustSupportRefIssuerSerial />
    <sp:MustSupportRefThumbprint />
    <sp:MustSupportRefEncryptedKey />
    <sp:RequireSignatureConfirmation />
  </wsp:Policy>
</sp:Wss11>
<sp:SignedParts>
  <sp:Body />
</sp:SignedParts>
<sp:EncryptedParts>
  <sp:Body />
</sp:EncryptedParts>
</wsp>All>
</wsp:ExactlyOne>
</wsp:Policy>

```

### SAMLToken with X509Token symmetric for message protection: 8.5.5.8

A SAML token is used for authentication. The SAML token in the request and the SOAP body in the request and response are signed and encrypted with X509Token symmetric message protection. There is also a message timestamp.

With X509Token symmetric protection, an ephemeral key is created to sign and encrypt the message. The ephemeral key is encrypted by using the receiver's public certificate.

In the following sample, the token reference is using a RequireThumbprintReference. You can change the policy to use a RequireIssuerSerialReference or RequireKeyIdentifierReference. You can also modify this policy to use derived keys from an ephemeral key to secure the message exchange by adding a <sp:RequireDerivedKeys /> assertion. This policy template is best used if the client can only use a SAML token to authenticate itself, and if the message exchange must be signed and encrypted.

The following policy shows a SAML token for authentication and X509Token symmetric for message protection:

```

<wsp:Policy wsu:Id="X509SymmetricForMessageAndSamlForClient">
  <wsp:ExactlyOne>
    <wsp>All>
      <sp:SignedEncryptedSupportingTokens
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
        <wsp:Policy>
          <sp:SamlToken
            sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <wsp:Policy>
                <sp:WssSamlV20Token11/>
              </wsp:Policy>
            </sp:SamlToken>
          </wsp:Policy>
        </sp:SignedEncryptedSupportingTokens>
        <sp:SymmetricBinding>
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:X509Token
                  sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/Never">
                    <wsp:Policy>
                      <sp:RequireThumbprintReference />
                      <sp:WssX509V3Token10 />
                    </wsp:Policy>
                  </sp:X509Token>
                </wsp:Policy>
              </sp:ProtectionToken>
            <sp:AlgorithmSuite>

```

```

    <wsp:Policy>
      <sp:Basic128 />
    </wsp:Policy>
  </sp:AlgorithmSuite>
  <sp:Layout>
    <wsp:Policy>
      <sp:Strict />
    </wsp:Policy>
  </sp:Layout>
  <sp:IncludeTimestamp />
  <sp:OnlySignEntireHeadersAndBody />
  <sp:EncryptSignature />
</wsp:Policy>
</sp:SymmetricBinding>
<sp:Wss11>
  <wsp:Policy>
    <sp:MustSupportRefKeyIdentifier />
    <sp:MustSupportRefIssuerSerial />
    <sp:MustSupportRefThumbprint />
    <sp:MustSupportRefEncryptedKey />
    <sp:RequireSignatureConfirmation />
  </wsp:Policy>
</sp:Wss11>
<sp:SignedParts>
  <sp:Body />
</sp:SignedParts>
<sp:EncryptedParts>
  <sp:Body />
</sp:EncryptedParts>
</wsp>All>
</wsp:ExactlyOne>
</wsp:Policy>

```

## Developing a password callback handler for WS-Security

**8.5.5.0**

In Liberty, password callback handlers can be used in many WS-Security scenarios to retrieve passwords. For example, passwords can be retrieved for generating UsernameTokens, opening keystores, or accessing private keys. A password callback handler is required for the provider when you use PasswordDigest. A password callback handler must be packaged as a user feature in Liberty.

### About this task

This task describes how to develop a password callback handler to retrieve user name and keystore key passwords.

### Procedure

1. Develop a password callback handler. The following example shows a callback handler:

```

package com.ibm.ws.wssecurity.example.cbh;

import java.util.HashMap;
import java.util.Map;
import javax.security.auth.callback.Callback;
import javax.security.auth.callback.CallbackHandler;
import org.apache.ws.security.WSPasswordCallback;

public class SamplePasswordCallback implements CallbackHandler {

    private Map<String, String> userPasswords = new HashMap<String, String>();
    private Map<String, String> keyPasswords = new HashMap<String, String>();
    public SamplePasswordCallback() {
        // some example user passwords
        userPasswords.put("user1", "user1pswd");
        userPasswords.put("admin", "adminpswd");
        // some example key passwords
        keyPasswords.put("alice", "keypswd");
        keyPasswords.put("bob", "keypswd");
    }
}

```

```

    }
    public void handle(Callback[] callbacks) throws IOException, UnsupportedOperationException {
        for (int i = 0; i < callbacks.length; i++) {
            WSPasswordCallback pwcb = (WSPasswordCallback)callbacks[i];
            String id = pwcb.getIdentifier();
            String pass = null;
            switch (pwcb.getUsage()) {
                case WSPasswordCallback.USERNAME_TOKEN_UNKNOWN:
                case WSPasswordCallback.USERNAME_TOKEN:
                    pass = userPasswords.get(id);
                    pwcb.setPassword(pass);
                    break;
                case WSPasswordCallback.SIGNATURE:
                case WSPasswordCallback.DECRYPT:
                    pass = keyPasswords.get(id);
                    pwcb.setPassword(pass);
                    break;
            }
        }
    }
}

```

2. Create a MANIFEST.MF file for the callback handler. The following example shows a MANIFEST.MF file:

```

Manifest-Version: 1.0
Bnd-LastModified: 1359415594428
Build-Identifier: SNAPSHOT-Mon Jan 28 17:26:34 CST 2013
Bundle-Copyright: The Program materials contained in this file are IBM
copyright materials. 5724-I63, 5724-J08, 5724-H89, 5724-H88, 5655-W65
Copyright International Business Machines Corp. 1999, 2012 All Rights
Reserved * Licensed Materials - Property of IBM US Government Users
Restricted Rights - Use, duplication or disclosure restricted by GSA ADP
Schedule Contract with IBM Corp.
Bundle-Description: An PasswordCallbackHandler; version=1.0.0
Bundle-ManifestVersion: 2
Bundle-Name: wssecuritycbh
Bundle-SymbolicName: com.ibm.ws.wssecurity.example.cbh
Bundle-Vendor: IBM
Bundle-Version: 1.0.0
Created-By: 1.6.0 (IBM Corporation)
Export-Package: com.ibm.ws.wssecurity.example.cbh;uses="com.ibm.websphe
re.ras.annotation,java.security.auth.callback";version="1.0.0"
Import-Package: com.ibm.websphere.ras,com.ibm.websphere.ras.annotation,c
om.ibm.ws.ffdc,java.security.auth.callback,org.apache.ws.security;version="[1.6,2)"
Require-Capability: osgi.ee;filter="(&(osgi.ee=JavaSE)(version>=1.6))"
Tool: Bnd-2.1.0.20120920-170235
WS-TraceGroup: WSSecurity

```

3. Package the callback handler into a JAR file. Create a JAR file with the callback handler class and the MANIFEST.MF file that you created in the previous steps. The following example shows the contents of a sample JAR file that is called SampleCbh.jar:

```

META-INF/MANIFEST.MF
com/ibm/ws/wssecurity/example/cbh/SamplePasswordCallback.class

```

4. Create a feature manifest file. The following example shows a sample feature manifest file that is called wssecdbh-1.0.mf:

```

Subsystem-ManifestVersion: 1
Subsystem-SymbolicName: wssecdbh-1.0; visibility:=public
Subsystem-Version: 1.0.0
Subsystem-Content: com.ibm.ws.wssecurity.example.cbh; version="[1,1.0.100)";
    location="lib/"; type="osgi.bundle"; start-phase:=APPLICATION_EARLY

```

```

Subsystem-Type: osgi.subsystem.feature
IBM-Feature-Version: 2

```

```

IBM-API-Package: com.ibm.ws.wssecurity.example.cbh; version="1.0"; type="internal"

```

5. Install the callback handler as a user feature in Liberty. Copy the callback handler JAR file and the feature manifest file to the Liberty user directory. The following example shows where to copy the files:

```
build.image/wlp/usr/extension/lib/SampleCbh.jar  
build.image/wlp/usr/extension/lib/features/wssecbh-1.0.mf
```

6. Configure the callback handler as a user feature in the `server.xml` file. Define the callback handler as a user feature in the `server.xml` file. The following example shows how to define the callback handler as a user feature:

```
<featureManager>  
  <feature>usr:wssecbh-1.0</feature>  
  <feature>servlet-3.0</feature>  
  <feature>appSecurity-2.0</feature>  
  <feature>jaxws-2.2</feature>  
  <feature>wsSecurity-1.1</feature>  
</featureManager>
```

## Results

You successfully developed the password callback handler and installed the callback handler to Liberty.

## What to do next

You can now use this callback handler to retrieve passwords for UsernameTokens and private keys that are used in WS-Security configuration.

## Securing a web service by using a WS-Security policy

0.5.5.0

You can develop and secure a Java API for XML Web Services (JAX-WS) web service by using a WS-Security policy in the IBM WebSphere Application Server Liberty. The examples are provided as a tutorial to explain the general steps that are involved in developing and securing a web service in Liberty. Do not use the examples in a production environment. Review your own security requirements to develop the Web Services Description Language (WSDL) contract and the WS-Security policy for protecting your web service applications.

## About this task

This task describes how to develop a simple JAX-WS web service application and secure the application by using a WS-Security policy.

This task uses two keystores: `enc-sender.jceks` and `enc-receiver.jceks`. These are WS-Security sample keystores that are shipped in traditional. If you have access to a traditional installation, you can obtain the sample keystores from one of the following directories:

```
profile_root/etc/ws-security/samples
```

```
WASHOME/profileTemplates/defaultdocuments/etc/ws-security/samples
```

If you do not have access to traditional, a zip file that contains all of the WS-Security sample keystores can be found here: <http://www-01.ibm.com/support/docview.wss?uid=swg21507405&aid=1>

## Procedure

1. Create the WSDL contract and WS-Security policy. In this sample, a WSDL contract with a WS-Security policy for a JAX-WS web service provider application is created. The WS-Security policy template called UsernameToken with X509Token asymmetric message protection (mutual authentication) is used. The client signs and encrypts the SOAP body and signs and encrypts the

UsernameToken in the request message. In the response message, the provider signs and encrypts the SOAP body. For a complete description of the security constraints in this example, see UsernameToken with X509Token asymmetric message protection (mutual authentication).

a. Create a WSDL contract for your service. The following example shows a sample WSDL contract:

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:wSDL="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:tns="http://com.ibm/was/wssample/sei/echo/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" name="WSSampleSei"
  targetNamespace="http://com.ibm/was/wssample/sei/echo/">
  <wsdl:types>
    <xsd:schema targetNamespace="http://com.ibm/was/wssample/sei/echo/"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <xsd:element name="echoStringResponse">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="echoResponse" type="xsd:string" />
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="echoStringInput">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="echoInput" type="xsd:string" />
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
    </xsd:schema>
  </wsdl:types>
  <wsdl:message name="echoOperationRequest">
    <wsdl:part element="tns:echoStringInput" name="parameter" />
  </wsdl:message>
  <wsdl:message name="echoOperationResponse">
    <wsdl:part element="tns:echoStringResponse" name="parameter" />
  </wsdl:message>
  <wsdl:portType name="EchoServicePortType">
    <wsdl:operation name="echoOperation">
      <wsdl:input message="tns:echoOperationRequest" />
      <wsdl:output message="tns:echoOperationResponse" />
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="EchoISOAP" type="tns:EchoServicePortType">
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="echoOperation">
      <soap:operation soapAction="echoOperation" style="document" />
      <wsdl:input>
        <soap:body use="literal" />
      </wsdl:input>
      <wsdl:output>
        <soap:body use="literal" />
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="Echo1Service">
    <wsdl:port binding="tns:EchoISOAP" name="Echo1ServicePort">
      <soap:address location="http://localhost:8010/WSSampleSei/Echo1Service" />
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

b. Add the namespaces that are needed to support the security policy to your WSDL in the wsdl:definitions element. The following example shows the added namespaces:

```
xmlns:wsp="http://www.w3.org/ns/ws-policy"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"
xmlns:sp13="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200802"
xmlns:wsaws="http://www.w3.org/2005/08/addressing"
```

c. Add the WS-Security policy fragment to your WSDL just before the wsdl:binding element. The policy template from UsernameToken with X509Token asymmetric message protection (mutual authentication) is used in this example.

d. Add a wsp:PolicyReference for your security policy to your wsdl:binding element. The following example shows the wsp:PolicyReference:

```
<wsp:PolicyReference URI="#AsymmetricX509MutualAuthenticationWithUnt" />
```

e. Verify that your final WSDL looks like the example. The following example shows the final WSDL:

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:tns="http://com.ibm/was/wssample/sei/echo/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" name="WSSampleSei"
  xmlns:wsp="http://www.w3.org/ns/ws-policy"
  xmlns:wssu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
  xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"
  xmlns:sp13="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200802"
  xmlns:wsa="http://www.w3.org/2005/08/addressing"
  targetNamespace="http://com.ibm/was/wssample/sei/echo/">
  <wsdl:types>
    <xsd:schema targetNamespace="http://com.ibm/was/wssample/sei/echo/"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <xsd:element name="echoStringResponse">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="echoResponse" type="xsd:string" />
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="echoStringInput">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="echoInput" type="xsd:string" />
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
    </xsd:schema>
  </wsdl:types>
  <wsdl:message name="echoOperationRequest">
    <wsdl:part element="tns:echoStringInput" name="parameter" />
  </wsdl:message>
  <wsdl:message name="echoOperationResponse">
    <wsdl:part element="tns:echoStringResponse" name="parameter" />
  </wsdl:message>
  <wsdl:portType name="EchoServicePortType">
    <wsdl:operation name="echoOperation">
      <wsdl:input message="tns:echoOperationRequest" />
      <wsdl:output message="tns:echoOperationResponse" />
    </wsdl:operation>
  </wsdl:portType>
  <wsp:Policy wsu:Id="AsymmetricX509MutualAuthenticationWithUnt">
    <wsp:ExactlyOne>
      <wsp>All>
        <sp:SignedEncryptedSupportingTokens xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
          <wsp:Policy>
            <sp:UsernameToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
              <wsp:Policy>
                <sp:WssUsernameToken10 />
              </wsp:Policy>
            </sp:UsernameToken>
          </wsp:Policy>
        </sp:SignedEncryptedSupportingTokens>
        <sp:AsymmetricBinding>
          <wsp:Policy>
            <sp:InitiatorToken>
              <wsp:Policy>
                <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                  <wsp:Policy>
                    <sp:WssX509V3Token10 />
                    <sp:RequireIssuerSerialReference />
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:InitiatorToken>
            <sp:RecipientToken>
              <wsp:Policy>
                <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/Never">
                  <wsp:Policy>
                    <sp:WssX509V3Token10 />
                    <sp:RequireIssuerSerialReference />
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:RecipientToken>
          </wsp:Policy>
        </sp:AsymmetricBinding>
      </wsp>All>
    </wsp:ExactlyOne>
  </wsp:Policy>

```

```

        </sp:RecipientToken>
        <sp:Layout>
            <wsp:Policy>
                <sp:Strict />
            </wsp:Policy>
        </sp:Layout>
        <sp:IncludeTimestamp />
        <sp:OnlySignEntireHeadersAndBody />
        <sp:EncryptSignature />
        <sp:AlgorithmSuite>
            <wsp:Policy>
                <sp:Basic128 />
            </wsp:Policy>
        </sp:AlgorithmSuite>
    </wsp:Policy>
</sp:AsymmetricBinding>
<sp:Wss11>
    <wsp:Policy>
        <sp:MustSupportRefKeyIdentifier />
        <sp:MustSupportRefIssuerSerial />
        <sp:MustSupportRefThumbprint />
        <sp:MustSupportRefEncryptedKey />
        <sp:RequireSignatureConfirmation />
    </wsp:Policy>
</sp:Wss11>
<sp:SignedParts>
    <sp:Body />
</sp:SignedParts>
<sp:EncryptedParts>
    <sp:Body />
</sp:EncryptedParts>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>
<wsdl:binding name="Echo1SOAP" type="tns:EchoServicePortType">
    <wsp:PolicyReference URI="#AsymmetricX509MutualAuthenticationWithUnt" />
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="echoOperation">
        <soap:operation soapAction="echoOperation" style="document" />
        <wsdl:input>
            <soap:body use="literal" />
        </wsdl:input>
        <wsdl:output>
            <soap:body use="literal" />
        </wsdl:output>
    </wsdl:operation>
</wsdl:binding>
<wsdl:service name="Echo1Service">
    <wsdl:port binding="tns:Echo1SOAP" name="Echo1ServicePort">
        <soap:address location="http://localhost:8010/WSSampleSei/Echo1Service" />
    </wsdl:port>
</wsdl:service>
</wsdl:definitions>

```

2. Create the web service application by using WSDL. This step can be done before or after the WS-Security policy is added to the WSDL. You can use supported tools to create a JAX-WS web service application from the WSDL that was developed in the previous section.

The following example shows a web service application that is developed from the WSDL by using the Rational Application Developer (RAD) tool:

```

@javax.jws.WebService (endpointInterface="com.ibm.was.wssample.sei.echo.EchoServicePortType",
    targetNamespace="http://com.ibm.was.wssample/sei/echo/",
    serviceName="Echo1Service",
    wsdlLocation = "WEB-INF/wsdl/Echo.wsdl",
    portName="Echo1ServicePort")
public class Echo1SOAPImpl {

    public EchoStringResponse echoOperation(EchoStringInput parameter) {
        String strInput = (parameter == null ? "input_is_null" : parameter.getEchoInput() );
        try {
            com.ibm.was.wssample.sei.echo.EchoStringResponse strOutput = new EchoStringResponse();
            strOutput.setEchoResponse( "Echo1SOAPImpl>>" + strInput );
            return strOutput;
        } catch (java.lang.Exception ex) {
            ex.printStackTrace();
        }
    }
}

```

```

@WebService (name = "EchoServicePortType",
            targetNamespace = "http://com/ibm/was/wssample/sei/echo/")
@SOAPBinding (parameterStyle = SOAPBinding.ParameterStyle.BARE)
@XmlSeeAlso ({
    ObjectFactory.class
})

public interface EchoServicePortType {

    @WebMethod (action = "echoOperation")
    @WebResult (name = "echoStringResponse", targetNamespace = "http://com/ibm/was/wssample/sei/echo/", partName = "parameter")
    public EchoStringResponse echoOperation(
        @WebParam (name = "echoStringInput", targetNamespace = "http://com/ibm/was/wssample/sei/echo/", partName = "parameter")
        EchoStringInput parameter);

}

```

The following code shows a managed web service client that invokes a web service provider application:

```

@WebServlet("ClientServlet")
public class ClientServlet extends HttpServlet {

    @WebServiceRef (value=Echo1Service.class, wsdlLocation="Echo.wsdl")
    Echo1Service echo1Service;

    public ClientServlet() {
        super ();
    }

    protected void doGet(HttpServletRequest request,
                        HttpServletResponse response) throws ServletException, IOException {
        processRequest(request, response);
    }

    protected void doPost(HttpServletRequest request,
                        HttpServletResponse response) throws ServletException, IOException {
        processRequest(request, response);
    }

    private void processRequest(HttpServletRequest req,
                        HttpServletResponse resp) throws ServletException, IOException {

        String endpointURL = "http://localhost:8010/WSSampleSei/Echo1Service";

        Echo1ServicePortProxy proxy = new Echo1ServicePortProxy(echo1Service);
        proxy._getDescriptor().setEndpoint(endpointURL);

        echoParm = new ObjectFactory().createEchoStringInput();
        echoParm.setEchoInput("Hello");

        String retval = proxy.echoOperation(echoParm).getEchoResponse();
    }
}

```

The following example shows the file structure of the web service provider application war file:

```

WEB-INF/web.xml
WEB-INF/wsdl/Echo.wsdl
WEB-INF/classes/com/ibm/was/wssample/sei/echo/Echo1SOAPImpl.class
WEB-INF/classes/com/ibm/was/wssample/sei/echo/EchoServicePortType.class
WEB-INF/classes/com/ibm/was/wssample/sei/echo/EchoStringInput.class
WEB-INF/classes/com/ibm/was/wssample/sei/echo/EchoStringResponse.class
WEB-INF/classes/com/ibm/was/wssample/sei/echo/ObjectFactory.class
WEB-INF/classes/com/ibm/was/wssample/sei/echo/package-info.class

```

The following example shows the file structure of the web service client application war file:

```

WEB-INF/web.xml
WEB-INF/wsdl/Echo.wsdl
WEB-INF/classes/com/ibm/was/wssample/client/ClientServlet.class
WEB-INF/classes/com/ibm/was/wssample/client/SampleClient.class
WEB-INF/classes/com/ibm/was/wssample/sei/echo/Echo1Service.class
WEB-INF/classes/com/ibm/was/wssample/sei/echo/Echo1ServicePortProxy.class
WEB-INF/classes/com/ibm/was/wssample/sei/echo/EchoStringInput.class

```

```

WEB-INF/classes/com/ibm/was/wssample/sei/echo/EchoStringResponse.class
WEB-INF/classes/com/ibm/was/wssample/sei/echo/ObjectFactory.class
WEB-INF/classes/com/ibm/was/wssample/sei/echo/package-info.class

```

3. Develop the callback handler. You must develop a callback handler to retrieve the user name and keystore key passwords. The user name password is used when you generate the UsernameTokens. The keystore passwords are used for accessing the private keys in the keystore. The callback handler must return plaintext passwords and be packaged and installed as a Liberty user feature.

The following sample code illustrates a callback handler:

```

package com.ibm.ws.wsssecurity.example.cbh;

import java.util.HashMap;
import java.util.Map;
import javax.security.auth.callback.Callback;
import javax.security.auth.callback.CallbackHandler;
import org.apache.ws.security.WSPasswordCallback;

public class SamplePasswordCallback implements CallbackHandler {
    private Map<String, String> userPasswords = new HashMap<String, String>();
    private Map<String, String> keyPasswords = new HashMap<String, String>();
    public SamplePasswordCallback() {
        // some example user passwords
        userPasswords.put("user1", "user1pswd");
        userPasswords.put("admin", "adminpswd");
        // some example key passwords
        keyPasswords.put("alice", "keypswd");
        keyPasswords.put("bob", "keypswd");
    }
    public void handle(Callback[] callbacks) throws IOException, UnsupportedCallbackException {
        for (int i = 0; i < callbacks.length; i++) {
            WSPasswordCallback pwcb = (WSPasswordCallback)callbacks[i];
            String id = pwcb.getIdentifier();
            String pass = null;
            switch (pwcb.getUsage()) {
                case WSPasswordCallback.USERNAME_TOKEN_UNKNOWN:
                case WSPasswordCallback.USERNAME_TOKEN:
                    pass = userPasswords.get(id);
                    pwcb.setPassword(pass);
                    break;
                case WSPasswordCallback.SIGNATURE:
                case WSPasswordCallback.DECRYPT:
                    pass = keyPasswords.get(id);
                    pwcb.setPassword(pass);
                    break;
            }
        }
    }
}

```

The following example shows the MANIFEST.MF file that is packaged with the callback handler:

```

Manifest-Version: 1.0
Bnd-LastModified: 1359415594428
Build-Identifier: SNAPSHOT-Mon Jan 28 17:26:34 CST 2013
Bundle-Copyright: The Program materials contained in this file are IBM
copyright materials. 5724-I63, 5724-J08, 5724-H89, 5724-H88, 5655-W65
Copyright International Business Machines Corp. 1999, 2012 All Rights
Reserved * Licensed Materials - Property of IBM US Government Users
Restricted Rights - Use, duplication or disclosure restricted by GSA ADP
Schedule Contract with IBM Corp.
Bundle-Description: An PasswordCallbackHandler; version=1.0.0
Bundle-ManifestVersion: 2
Bundle-Name: wsssecuritycbh
Bundle-SymbolicName: com.ibm.ws.wsssecurity.example.cbh
Bundle-Vendor: IBM
Bundle-Version: 1.0.0
Created-By: 1.6.0 (IBM Corporation)
Export-Package: com.ibm.ws.wsssecurity.example.cbh;uses:="com.ibm.websphe
re.ras.annotation,javax.security.auth.callback";version="1.0.0"
Import-Package: com.ibm.websphere.ras,com.ibm.websphere.ras.annotation,c

```

```
om.ibm.ws.ffdc, javax.security.auth.callback, org.apache.ws.security; version="[1.6,2)"
Require-Capability: osgi.ee; filter:="(&(osgi.ee=JavaSE)(version>=1.6))"
Tool: Bnd-2.1.0.20120920-170235
WS-TraceGroup: WSSecurity
```

- a. Create a JAR file with the callback handler and the feature manifest file - wssecdbh-1.0.mf. Create a JAR file that is called SampleCbh.jar with the following contents:

```
META-INF/MANIFEST.MF
com/ibm/ws/wssecurity/example/cbh/SamplePasswordCallback.class
```

The following example shows the wssecdbh-1.0.mf file:

```
Subsystem-ManifestVersion: 1
Subsystem-SymbolicName: wssecdbh-1.0; visibility:=public
Subsystem-Version: 1.0.0
Subsystem-Content: com.ibm.ws.wssecurity.example.cbh; version="[1,1.0.100)";
    location:="lib/"; type="osgi.bundle"; start-phase:=APPLICATION_EARLY
```

```
Subsystem-Type: osgi.subsystem.feature
IBM-Feature-Version: 2
```

```
IBM-API-Package: com.ibm.ws.wssecurity.example.cbh; version="1.0"; type="internal"
```

- b. Copy the callback handler JAR file and the feature manifest file under the Liberty user directory. The following example shows where the callback handler JAR file and the feature manifest file are copied:

```
build.image/wlp/usr/extension/lib/SampleCbh.jar
build.image/wlp/usr/extension/lib/features/wssecdbh-1.0.mf
```

4. Configure WS-Security in the Liberty server. Enable the WS-Security feature in the Liberty server configuration file: server.xml and configure WS-Security for the sample web service client and provider application that is developed in the previous sections.

The following example shows how to configure WS-Security:

```
<server>
  <featureManager>
    <feature>usr:wssecdbh-1.0</feature>
    <feature>servlet-3.0</feature>
    <feature>appSecurity-2.0</feature>
    <feature>jsp-2.2</feature>
    <feature>jaxws-2.2</feature>
    <feature>wsSecurity-1.1</feature>
  </featureManager>
  <basicRegistry id="basic" realm="customRealm">
    <user name="user1" password="user1pswd" />
    <user name="user2" password="user2pswd" />
  </basicRegistry>
  <wsSecurityProvider id="default"
    ws-security.callback-handler="com.ibm.ws.wssecurity.example.cbh.SamplePasswordCallback"
    ws-security.signature.username="bob">
    <signatureProperties org.apache.ws.security.crypto.merlin.keystore.type="jceks"
      org.apache.ws.security.crypto.merlin.keystore.password="storepswd"
      org.apache.ws.security.crypto.merlin.keystore.alias="bob"
      org.apache.ws.security.crypto.merlin.file="{server.config.dir}/enc-receiver.jceks" />
    <encryptionProperties org.apache.ws.security.crypto.merlin.keystore.type="jceks"
      org.apache.ws.security.crypto.merlin.keystore.password="storepswd"
      org.apache.ws.security.crypto.merlin.keystore.alias="alice"
      org.apache.ws.security.crypto.merlin.file="{server.config.dir}/enc-receiver.jceks" />
  </wsSecurityProvider>
  <wsSecurityClient id="default"
    ws-security.password="security"
    ws-security.username="user1"
    ws-security.callback-handler="com.ibm.ws.wssecurity.example.cbh.SamplePasswordCallback"
    ws-security.encryption.username="alice">
    <signatureProperties org.apache.ws.security.crypto.merlin.keystore.type="jceks"
      org.apache.ws.security.crypto.merlin.keystore.password="storepswd"
      org.apache.ws.security.crypto.merlin.keystore.alias="alice"
      org.apache.ws.security.crypto.merlin.file="{server.config.dir}/enc-sender.jceks"/>
    <encryptionProperties org.apache.ws.security.crypto.merlin.keystore.type="jceks"
      org.apache.ws.security.crypto.merlin.keystore.password="storepswd"
      org.apache.ws.security.crypto.merlin.keystore.alias="bob"
      org.apache.ws.security.crypto.merlin.file="{server.config.dir}/enc-sender.jceks" />
  </wsSecurityClient>
</server>
```



```

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <wsse:SecurityTokenReference
    xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
    xmlns:wss11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
    wss11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey">
    <wsse:Reference URI="#EK-B1165B2A578AFFC7D61364959566705"></wsse:Reference>
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
<xenc:CipherData>
  <xenc:CipherValue>...</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
</soap:Body>
</soap:Envelope>

```

The following example shows a SOAP response message:

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
      xmlns:wssu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
      soap:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="TS-7">
        <wsu:Created>2013-04-03T03:26:07.286Z</wsu:Created>
        <wsu:Expires>2013-04-03T03:31:07.286Z</wsu:Expires>
      </wsu:Timestamp>
      <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="EK-B1165B2A578AFFC7D613649595673129">
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"></xenc:EncryptionMethod>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <wsse:SecurityTokenReference>
            <ds:X509Data>
              <ds:X509IssuerSerial>
                <ds:X509IssuerName>CN=Alice,O=IBM,C=US</ds:X509IssuerName>
                <ds:X509SerialNumber>24054530212598</ds:X509SerialNumber>
              </ds:X509IssuerSerial>
            </ds:X509Data>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
        <xenc:CipherData>
          <xenc:CipherValue>...</xenc:CipherValue>
        </xenc:CipherData>
        <xenc:ReferenceList>
          <xenc:DataReference URI="#ED-10"></xenc:DataReference>
          <xenc:DataReference URI="#ED-11"></xenc:DataReference>
          <xenc:DataReference URI="#ED-12"></xenc:DataReference>
        </xenc:ReferenceList>
      </xenc:EncryptedKey>
      <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        Id="ED-12"
        Type="http://www.w3.org/2001/04/xmlenc#Element">
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></xenc:EncryptionMethod>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <wsse:SecurityTokenReference
            xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
            xmlns:wss11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
            wss11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey">
            <wsse:Reference URI="#EK-B1165B2A578AFFC7D613649595673129"></wsse:Reference>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
        <xenc:CipherData>
          <xenc:CipherValue>...</xenc:CipherValue>
        </xenc:CipherData>
      </xenc:EncryptedData>
      <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        Id="ED-11"
        Type="http://www.w3.org/2001/04/xmlenc#Element">
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></xenc:EncryptionMethod>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <wsse:SecurityTokenReference
            xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
            xmlns:wss11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
            wss11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey">
            <wsse:Reference URI="#EK-B1165B2A578AFFC7D613649595673129"></wsse:Reference>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
        <xenc:CipherData>
          <xenc:CipherValue>...</xenc:CipherValue>
        </xenc:CipherData>
      </xenc:EncryptedData>
    </wsse:Security

```

```

</SOAP-ENV:Header>
<soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
  wsu:Id="Id-2035943749">
  <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    Id="ED-10"
    Type="http://www.w3.org/2001/04/xmlenc#Content">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></xenc:EncryptionMethod>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <wsse:SecurityTokenReference
        xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
        xmlns:wss11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
        wss11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey">
        <wsse:Reference URI="#EK-B1165B2A578AFFC7D613649595673129"></wsse:Reference>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>...</xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</soap:Body>
</soap:Envelope>

```

## What to do next

You can now develop your own WSDL file and protect the web service application by using a WS-Security policy that matches your security requirements.

## Migrating CXF WS-Security to Liberty

**8.5.5.0**

Migrating CXF WS-Security to Liberty is easy and straightforward. The migration work includes migrating the Spring or Spring-like configuration to the `server.xml` file. If a `CallbackHandler` is required, you must also package and install a password `CallbackHandler` as a Liberty user feature.

### Before you begin

Ensure that you have a working knowledge of CXF WS-Security enabled web services outside Liberty.

### About this task

To protect your web service application with WS-Security, your JAX-WS application must contain a `wsdl` that has an embedded WS-Security policy. There must be a `PolicyReference` to the embedded WS-Security policy in either the `wsdl:binding` or `wsdl:operation` sections or both. After you migrate your web service to Liberty, you can enable a WS-Security policy-driven WS-Security configuration. This task describes how you can migrate an Apache CXF WS-Security configuration to Liberty.

### Procedure

1. Add the `wsSecurity-1.1` feature to the `server.xml` file to enable WS-Security in Liberty.
2. Add the WS-Security configuration to the `server.xml` file. CXF WS-Security in Liberty does not support the Spring configuration file, or its equivalent configuration file from other vendors. You must migrate extra configurations that are defined outside the policy from the Spring or its equivalent configuration file to the `server.xml` file in Liberty.

Create the `<wsSecurityClient>` element to hold the client-side configuration, and the `<wsSecurityProvider>` element to hold the server-side configuration. All configuration property name and value pairs from CXF and WSS4J must be preserved. You can use the same name and value pairs from the Spring or equivalent configuration files. For crypto properties, you must create the `<signatureProperties>` and `<encryptionProperties>` subelements to hold all the required properties. For more information, see [Web services security default configuration](#).

3. Package your password callback handler as a Liberty profile user feature if you have a password callback handler in your Spring configuration files. For more information about the password `CallbackHandler`, see [Developing a password callback handler for WS-Security](#).

## Results

You migrated a WSDL-first web service to Liberty.

## Authenticate web service clients with a SAML (Security Markup Assertion Language) Token

8.5.5.8

Web Services Security SAML Token Profile 1.1 defines how to use Security Assertion Markup Language (SAML) V1.1 and V2.0 assertions with the Web Services Security (WSS): SOAP Message Security V1.1 specification. Liberty supports Web Services Security SAML Token Profile 1.1 for SAML v2.0 assertion with bearer confirmation method.

### About this task

Liberty supports SAML v2.0 with bearer confirmation method (<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">). A web services client propagates a SAML token to the web services provider as a means of identifying the requester, and the web services provider can use this SAML token information to authenticate the requester.

The requirement of a SAML token is expressed as one of the supporting tokens in the WS-Security policy. You can add a SamlToken requirement as a required token in one of the supporting token assertions, including SupportingTokens, SignedSupportingTokens, SignedEncryptedSupportingTokens, and EncryptedSupportingTokens.

### Procedure

1. Configure a web services client to propagate the SAML token.

It is required that a Saml20Token (com.ibm.websphere.security.saml2.Saml20Token) exists in the RunAs Subject. If a SamlToken policy assertion is configured, the Liberty WS-Security runtime will automatically extract the Saml20Token from the RunAs Subject, and attach a SAML assertion to the <wsse:Security> SOAP header. The following steps are required:

- a. Add wsSecuritySaml-1.1 to the featureManager in the server.xml file.

```
<featureManager>
  <feature>wsSecuritySaml-1.1</feature>
</featureManager>
```

- b. The application must specify the SAML token as a supporting token (including SupportingTokens, SignedSupportingTokens, SignedEncryptedSupportingTokens, and EncryptedSupportingTokens token assertion) in the policy in the .wsdl file.

```
<wsp:Policy wsu:Id="CallerHttpPolicy">
  <sp:SupportingTokens>
    <wsp:Policy>
      <sp:SamlToken
        sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
        <wsp:Policy>
          <sp:WssSamlV20Token11 />
        </wsp:Policy>
      </sp:SamlToken>
    </wsp:Policy>
  </sp:SupportingTokens>
</wsp:Policy>
```

2. Authenticate the Web Service with a SAML token.

When the web services provider receives the SOAP message with the SAML token, it validates the token first and then uses the SAML token attributes to complete the authentication process. The following are the steps that are involved in validating the SAML token:

- a. Add wsSecuritySaml-1.1 to the featureManager in the server.xml file.

```

<featureManager>
  <feature>wsSecuritySaml-1.1</feature>
</featureManager>

```

- b. The application must specify the SAML token as a supporting token in the policy inside the .wsdl file.
- c. The following attributes in the server configuration are used when validating the token.

```

<wsSecurityProvider id="default"
  ..
  ..
  <saml token
    wantAssertionsSigned="true"
    clockSkew="5m"
    timeToLive="30m"
    requiredSubjectConfirmationMethod="bearer"
    audienceRestrictions="https://../aud1"
    audienceRestrictions="aud2" .. />

</wsSecurityProvider>

```

- wantAssertionsSigned - Specify whether the <saml:Assertion> element in the SOAP message received by the WS-Security provider is signed.
- clockSkew - The time difference that is allowed between systems that generated the SAML token and received the SAML token. The default is 5 minutes.
- timeToLive - The life time of a SAML Assertion. This setting is required when the NoOnOrAfter condition is missing in the SAML assertion. The default is 30 minutes.
- requiredSubjectConfirmationMethod - Subject confirmation method in the SAML assertion. The default is bearer.
- audienceRestrictions - The allowed audiences of the SAML assertion. The default is all audiences allowed.

For further details on the steps involved in authenticating, see *Creating a WS-Security SAML caller configuration*.

## Web Services Security HTTPS transport policy assertions

### 8.5.5.0

You can use assertions in the Web Services Security (WS-Security) policy defined in the WSDL file to ensure that SOAP messages are protected with the HTTPS secure transport. When used with security tokens such as UsernameTokens with clear text passwords, HTTPS can help to ensure confidentiality.

The assertions for the HTTPS transport in the WS-Security policy do not set up the HTTPS transport between the requestor and provider. They ensure only that the HTTPS transport is used when the web services application with the defined policy is called. **8.5.5.0** To enable the transport security for web services, see “Securing web services at the transport level” on page 2018.

Ensure that HTTPS is set up between the web services client and provider. To protect your SOAP messages with the HTTPS secure transport, complete the following extra steps.

1. **8.5.5.0** WS-Security must be explicitly enabled by adding the wsSecurity-1.1 feature. Make sure you also add the appSecurity-2.0, servlet-3.0(or servlet-3.1) and jaxws-2.2 features, and other required Liberty features to the server.xml file of the Liberty profile.
2. The WS-Security policy attached to your web services application must include a TransportBinding assertion, and must match the HTTPS configuration. The following example illustrates a sample TransportBinding assertion:

```

<wsp:Policy xmlns:wsp="..." xmlns:sp="...">
  <sp:TransportBinding>
    <wsp:Policy>
      <sp:TransportToken>
        <wsp:Policy>
          <sp:HttpsToken />
        </wsp:Policy>
      </sp:TransportToken>
      <sp:AlgorithmSuite>
        <wsp:Policy>
          <sp:Basic256 />
        </wsp:Policy>
      </sp:AlgorithmSuite>
      <sp:Layout>
        <wsp:Policy>
          <sp:Strict />
        </wsp:Policy>
      </sp:Layout>
      <sp:IncludeTimestamp />
    </wsp:Policy>
  </sp:TransportBinding>
</wsp:Policy>

```

By completing these extra steps after the HTTPS configuration, SOAP messages are required to be sent over HTTPS from a web services client to a web services provider.

---

## Liberty:Security considerations

### 8.5.6.0

Consider the following when you configure Security for Liberty.

#### LTPA

- Protect file access to the LTPA keys file because it contains the cryptographic material that is used to encrypt and decrypt the user data. Ensure that only the server and administrators have access to this file.
- Ensure that all servers use the same LTPA keys. In addition, make sure that the all the servers have their time and date synchronized.
- When you specify a password, ensure that it is the same password for all servers that use the same set of LTPA keys. The password is not used to generate the keys, but rather it is used to encrypt the LTPA keys file to prevent the keys from being read. If you copy the LTPA keys file to another Liberty server to achieve Single Sign-On (SSO), the password is required to gain access to the keys in the LTPA keys file. For more information about LTPA, see Configuring LTPA on Liberty topic.

#### Passwords

- Encrypt passwords by using the securityUtility encode command.
- If you override the default encryption key with the wlp.password.encryption.key property, set the property in a separate configuration file that is stored outside the normal configuration directory for the server.

#### Authorization

- If you specify an auth-constraint with no roles in an application, then no one is allowed to access the resource.
- Be cautious when you specify the EVERYONE special subject, as this specification is equivalent to not protecting a resource.

## Authentication

- The timeout value for the authentication cache that is specified in the <authCache> element must be smaller than the expiration value for the LTPA token that is specified in the <ltpa> element.

---

## Securing Liberty by using HTTP Strict Transport Security (HSTS)

You can secure Liberty by first setting up HTTP Strict Transport Security (HSTS) in IBM HTTP Server. Then, add IBM HTTP Server as a front end to Liberty so that connections between Liberty and a client are over HTTPS.

### Procedure

1. Set up HSTS in IBM HTTP Server.
2. Add IBM HTTP Server as a front end to Liberty.



---

## Chapter 9. Developing applications in the Liberty environment

WebSphere Application Server Liberty is a lightweight, composable application server that provides a convenient application development environment for your web and OSGi applications. Applications that run on Liberty also run on the WebSphere Application Server traditional server.

### About this task

Liberty simplifies application development by providing the following key benefits and more:

- Frictionless download, at no cost, for development purposes
- Ultra lightweight modular runtime environment, with an install size of under 50 MB
- Very fast startup time; for example, less than 5 seconds for simple web applications
- Simplified configuration for quick time to productivity
- Java EE and OSGi application deployment support for web applications
- LDAP registry support
- Deployment, as a package, of an application and configured server
- Managed, centralized deployment of a packaged application and server
- Availability of WebSphere Application Server Developer Tools as Eclipse plug-ins for broad tools support
- Platform support for distributed platforms, z/OS, and Mac OS

Very fast restart times, coupled with its small size, dynamic behavior, and ease of use, make Liberty a good option for developers building web applications that do not require the full Java EE environment of traditional enterprise application server profiles. Familiar WebSphere Application Server enterprise qualities of service, such as security and transaction integrity, are enabled as required.

---

### Developing applications that interact with z/OS resources



To interact between Liberty applications and resources in your z/OS environment, you can use features such as z/OS Connect and the optimized local adapters.

### Developing applications that use optimized local adapters on Liberty



Optimized local adapters enable high-performance calling between native-language applications on z/OS and business logic in a Liberty server environment.

### Using Liberty to Invoke an API to call an enterprise bean from an external address space



Use the WebSphere optimized local adapter (WOLA) Invoke API to call from an external address space to a stateless session bean that is deployed on a local Liberty server for z/OS.

## Before you begin

To identify your enterprise bean as a potential target of an optimized local adapter call, your Enterprise JavaBean (EJB) application must implement the `com.ibm.websphere.ola.ExecuteLocalBusiness` interface as a local business interface. The interface is located in the `wlp/dev/api/ibm/com.ibm.websphere.appserver.api.zosLocalAdapters_1.0.0.jar` file.

The Liberty server must be active on the same z/OS image that the register request originates from. Ensure that the current address space is already registered and bound to the target optimized local adapter group using the Register API. For more information about registering an external address space, see “Registering an external address space with a local Liberty server using optimized local adapters” on page 1711.

## About this task

This method of calling an enterprise bean provides a simplified path for when you know the response area length before you call the bean. If you do not know the response area length or want more flexibility when you call the bean, see “Using the Liberty optimized local adapters APIs to invoke an enterprise bean from an external address space” on page 2075.

## Procedure

1. Decide which parameters to use when you call the bean using the Invoke API, which is BBOA1INV.

The API accepts parameters for the following items:

- The register name that you specified when you called the Register API
- The request type, which must be set to 1 for local EJB work requests
- The name of the service to invoke, which must be the Java Naming and Directory Interface (JNDI) local business interface path name of the stateless session bean
- The length of the service name
- A pointer to the address of the start of the request data to send
- The length of the request data to send
- A pointer to the address of the start of the response data area
- The length of the response data to send
- The number of seconds until the connection times out

For more information about API parameters, see “Optimized local adapters APIs on Liberty for z/OS” on page 2079.

2. Call the Invoke API for your caller with your selected parameters from a native-language application in the client address space. In the target Enterprise JavaBeans (EJB) application, the execute method runs and then starts any business logic that is required before returning the response data as a serialized byte array back to the native-language caller.
3. Review the response data. A 0 return code and reason code indicates that the client Invoke API call completed successfully and the response data and response data length are saved in the areas designated by the caller.
4. The client application repeats these steps using the same register name call, calling as many stateless session beans as needed, as often as needed.

**Attention:** With the Invoke API, the three primitive functions, `Send_Request`, `Receive_RespLen`, and `Get_Data` are all completed. The calling thread is blocked until the response data is received and copied to the response area.

## Results

The client starts a stateless session bean from the Liberty server using the optimized local adapter Invoke API.

## Using the Liberty optimized local adapters APIs to invoke an enterprise bean from an external address space

z/OS



8.5.5.2

Use the WebSphere optimized local adapter (WOLA) APIs to connect an external address space to a Liberty server and invoke a local stateless session bean.

### Before you begin

To identify your enterprise bean as a potential target of an optimized local adapter call, your Enterprise JavaBean (EJB) application must implement the `com.ibm.websphere.ola.ExecuteLocalBusiness` interface as a local business interface. The interface is located in the `wlp/dev/api/ibm/com.ibm.websphere.appserver.api.zosLocalAdapters_1.0.0.jar` file.

For programs that are running under Customer Information Control System (CICS), the optimized local adapters task-related user exist (TRUE) program must be activated before a connection is made between CICS and the Liberty server. For more information, see “Liberty server transactions for CICS: BBOC, BBO\$, and BBO#” on page 1705.

The Liberty server must be active on the same z/OS image that the register request originates from. Ensure that the current address space is already registered and bound to the target optimized local adapter group using the Register API. For more information about registering an external address space, see “Registering an external address space with a local Liberty server using optimized local adapters” on page 1711.

### About this task

This method of invoking a stateless session bean provides more flexibility and is for situations when you might not know the response area maximum length before you call. For a simplified method of invoking the bean when the response area length is known, see “Using Liberty to Invoke an API to call an enterprise bean from an external address space” on page 2073.

### Procedure

1. Call the Connection Get API, `BBOA1CNG`, from the native-language application in the client address space, passing the register name that you used when you called the Register API, `BBOA1REG`. The call returns a connection handle that must be used for all future API calls.
2. Call the Send Request API, `BBOA1SRQ`, from the native-language application in the client address space. For the **requestservicename** parameter, specify the Java Naming and Directory Interface (JNDI) local business interface path name for the enterprise bean that you want to invoke. Use the JNDI name in the global JNDI namespace. The Liberty server then invokes the execute method for the local business interface that the EJB application implements.

If you set the Send Request API **async** parameter to 0, the API returns the response length and the return value. You can then directly call the Get Message Data API.

If you set the Send Request API **async** parameter to 1, control returns to the client application so you can call the Receive Response Length API.

3. If you called the Send Request API with the **async** parameter set to 1, call the Receive Response Length API, `BBOA1RCL`, setting the **async** parameter to 0 or 1. The client application uses the response length that is returned by Receive Response Length API to ensure that it has an area large enough to hold the response data.

If you set the Receive Response Length API **async** parameter to 0, the API blocks the thread until a response is received.

If you set the Receive Response Length API **async** parameter to 1, the API returns immediately regardless of whether it received a response.

4. Call the Get Message Data API, BBOA1GET, to copy the response data into the client application's buffer.
5. The client application can continue to send requests and receive message data using the same connection handle until it sends all requests and is ready to release the connection. To release the connection, the application calls the Connection Release API, BBOA1CNR. Connection handles must be released before they can be retained on a Connection Get API call and used again.

## Using the optimized local adapters to connect to an application in an external address space from a Liberty application



Use the WebSphere optimized local adapters (WOLA) APIs to connect to an application in an external address space from an application that is deployed on the Liberty server.

### Before you begin

Register the external address space with the WOLA group. For more information, see “Registering an external address space with a local Liberty server using optimized local adapters” on page 1711.

Set up the application in the external address space as an optimized local adapters server task by calling either the Receive Request Any, Receive Request Specific, or Host Service APIs. For more information, see “Optimized local adapters APIs on Liberty for z/OS” on page 2079.

### Procedure

1. Enable the Liberty Enterprise JavaBeans (EJB) application to access the connection factory by using either resource injection or a JNDI lookup.
  - For resource injection, use the @Resource annotation to reference the connection factory that you defined in the server.xml file. The following example references the eis/ola connection factory:
 

```
@Resource(lookup = "eis/ola",
            authenticationType = Resource.AuthenticationType.APPLICATION,
            shareable = false)
private ConnectionFactory cf;
```
  - For JNDI lookup, create a resource reference in your application that you then look up in the enterprise bean.
    - a. Create a resource reference in the META-INF/ibm-ejb-jar-bnd.xml file for the application, where the binding-name matches the JNDI name of the connection factory in the server.xml file.
 

```
<session name="HSCBC016Bean">
  <resource-ref name="eis/ola" binding-name="eis/ola"/>
</session>
```
    - b. In the EJB implementation, create a connection factory object that looks up the resource reference that you defined. Prefix the name of the resource reference with java:comp/env/ as shown in the following example:
 

```
Context ctx = new InitialContext();
ConnectionFactory cf = ctx.lookup("java:comp/env/eis/ola");
```
2. Create a connection specification by creating a ConnectionSpecImpl object. Provide the register name of the external address space that you want to connect to in either of the following ways:
  - Add the register name as an attribute on the connection factory
  - Call the ConnectionSpecImpl method, setRegisterName, with the register name

The following example creates the ConnectionSpecImpl object and provides the MyRES1 register name:

```
ConnectionSpecImpl csi = new ConnectionSpecImpl();
csi.setRegisterName ("MyRES1");
```
3. Create a connection with the connection factory, as shown in the following example:
 

```
Connection con = cf.getConnection(csi);
```

## Results

The Liberty application is connected to an external address space and can call services that are hosted on the external address space. For more information, see “Using the Liberty optimized local adapters APIs to call services in an external address space.”

## Using the Liberty optimized local adapters APIs to call services in an external address space



Use the WebSphere optimized local adapters (WOLA) APIs to call services on an external address space or subsystem from a Liberty server.

### Before you begin

Connect the application to an external address space or subsystem as described in “Using the optimized local adapters to connect to an application in an external address space from a Liberty application” on page 2076.

If you want to pass record data that is generated by the Rational Application Developer CICS/IMS Java Data Binding wizard, you must first enable the connection to use the generated record data. For more information, see “Enabling generated record data in outbound optimized local adapter connections in Liberty” on page 2078

### Procedure

1. In the application, create an interaction from the Connection object that you created. The following example creates the `int` interaction from the `con` Connection object:  

```
Interaction int = con.createInteraction();
```
2. Create an interaction specification by creating an `InteractionSpecImpl` object and providing the service name, which is the name of the method that you want to call in the external address space or subsystem. The service name must be the name that you set when you called the Receive Request Any, Receive Request Specific, or Host Service APIs, or, if you are using a Customer Information Control System (CICS) server task, the name of the CICS program. The following example provides the `MYSERVICE` service name on the `isi` `InteractionSpecImpl` object:  

```
InteractionSpecImpl isi = new InteractionSpecImpl();
isi.setServiceName("MYSERVICE");
```
3. Run the interaction with the interaction specification. The following example runs the `int` interaction with the `isi` interaction specification and sends no data:  

```
int.execute(isi, null);
```

### Example

The following example shows how to start an interaction with input and output data as a byte array (`byte[]`):

```
public byte[] driveInteraction(javax.resource.cci.ConnectionFactory cf,
    javax.resource.cci.Connection con,byte[] inputDataBytes),throws javax.resource.ResourceException
{
    // Create an interaction using the optimized local adapter connection
    javax.resource.cci.Interaction i = con.createInteraction();
    // The InteractionSpec describes the service we want to call
    com.ibm.websphere.ola.InteractionSpecImpl isi = new com.ibm.websphere.ola.InteractionSpecImpl();
    isi.setServiceName("MYSERVICE");
    // The input data is specified using an IndexedRecord. The first
    // slot in the indexed record contains the input data bytes.
    javax.resource.cci.RecordFactory rf = cf.getRecordFactory();
    javax.resource.cci.IndexedRecord ir = rf.createIndexedRecord(null);
    ir.add(inputDataBytes);
```

```

// The interaction returns another IndexedRecord, whose first
// slot contains the output data bytes.
javax.resource.cci.Record or = i.execute(isi, ir);
byte[] outputDataBytes = null;

if (or != null)
{
    outputDataBytes = (byte[])((javax.resource.cci.IndexedRecord)or).get(0);
}

// Return the output data to the caller
return outputDataBytes;
}

```

The following example shows how to start an interaction using a Rational Application Developer generated copybook Record object. .

```

/**
 * An example of driving an optimized local adapter interaction, using a Rational
 * Application Developer copybook mapping class as input (inputRecord) and receiving
 * a Rational Application Developer copybook mapping as output.
 */
public javax.resource.cci.Record driveInteraction(
    javax.resource.cci.Connection con,
    javax.resource.cci.Record inputRecord)
    throws javax.resource.ResourceException
{
    // Create an interaction using the OLA connection
    javax.resource.cci.Interaction i = con.createInteraction();
    // The InteractionSpec describes the service we want to call com.ibm.websphere.ola.InteractionSpecImpl isi =
    new com.ibm.websphere.ola.InteractionSpecImpl();
    isi.setServiceName("MYSERVICE");
    // The Rational Application Developer generated copybook implements
    // javax.resource.cci.Record and can be passed directly to the interaction.
    // The interaction returns an IndexedRecord, whose first slot contains
    // the output data bytes.
    javax.resource.cci.Record or = i.execute(isi, inputRecord);
    javax.resource.cci.Record outputRecord = null;
    if (or != null)
    {
        // In this example, RADGeneratedOutputType is the name of the Rational Application Developer
        // generated copybook mapping class.
        outputRecord = new RADGeneratedOutputType();
        // The output bytes are stored in the output record returned on the
        // interaction, which is an IndexedRecord.
        byte[] outputDataBytes =
            (byte[])((javax.resource.cci.IndexedRecord)or).get(0);

        // To convert the output bytes to another Rational Application Developer generated copybook,
        // call the setBytes(byte[]) method of that class. The class will
        // implement the com.ibm.etools.marshall.RecordBytes interface.
        ((com.ibm.etools.marshall.RecordBytes)outputRecord)
            .setBytes(outputDataBytes);
    }

    // Return the output data to the caller
    return outputRecord;
}

```

## Enabling generated record data in outbound optimized local adapter connections in Liberty: z/OS



### 8.5.5.2

If you are passing data by using one of the Java EE Connector Architecture (JCA) record interfaces that the WebSphere optimized local adapters (WOLA) support, you can generate the Record classes by using the Rational Application Developer CICS/IMS Java Data Binding wizard.

## About this task

You can use the Rational Application Developer CICS/IMS Java Data Binding wizard to generate a `javax.resource.cci.Record` object that can replace the byte array that sends and receives data in the `IndexRecordImpl` and `MappedRecordImpl` objects. To use the generated Record classes, you must set up an extra library in the Liberty server instance to enable the server instance to serialize and deserialize the data in the Record object.

## Procedure

1. Copy the marshalling JAR file from Rational Application Developer into a `lib` subdirectory underneath the server configuration directory, which contains the `server.xml` file. The licensed, redistributable `marshall.jar` file is located in the `com.ibm.ccl.commonj.connector.metadata_version.timestamp` plug-in in the `runtime` folder. The exact name of the plug-in folder varies depending on the Rational Application Developer version.
2. In the `server.xml` file, create a `library` element that points to the new location of the marshalling JAR file, as shown in the following example. Replace `marshall.jar` with the actual name of your marshalling JAR file.

```
<!-- Library required by RAD generated application classes. -->
<library id="MarshallLib">
  <file name="{server.config.dir}/lib/marshall.jar"/>
</library>
```

3. In the `server.xml` file, add the new library to the application definition that contains the generated Record class by specifying the library ID that you created on a `classloader` element. The following example adds the `MarshallLib` library to the `WolaApp` application.

```
<!-- Application installed in {server.config.dir}/apps. -->
<application id="WolaApp" name="WolaApp" location="OLA.ear">
  <classloader commonLibraryRef="MarshallLib"/>
</application>
```

## Results

You can now use the Rational Application Developer CICS/IMS Java Data Binding wizard to generate record data for your outbound connection. For more information, see “Using the Liberty optimized local adapters APIs to call services in an external address space” on page 2077.

## Optimized local adapters APIs on Liberty for z/OS



WebSphere optimized local adapters (WOLA) on Liberty are supported by a set of z/OS native-language callable services application programming interfaces (APIs) and the Java EE Connector Architecture (JCA).

You can use the callable services from the following native programming languages:

- Cobol
- C/C++
- PL/I
- High-level assembly languages

The term *local connection* refers to a cross-memory link that is created for communication between an external address space on the z/OS system and the Liberty server on the same z/OS system. The client address space must be running on the same z/OS image. The adapter API manages these local connections in pools that are associated with each uniquely registered caller. The 12-character registration name can be used for only one set of connection pools per address space. The number of unique registrations in a single address space is limited only by the amount of available storage.

The Liberty supports the following optimized local adapters APIs:

- Register - BBOA1REG
- Unregister - BBOA1URG
- Connection Get - BBOA1CNG
- Connection Release - BBOA1CNR
- Send Request - BBOA1SRQ
- Send Response - BBOA1SRP
- Send Response Exception - BBOA1SRX
- Receive Request Any - BBOA1RCA
- Receive Request Specific - BBOA1RCS
- Receive Response Length - BBOA1RCL
- Get Message Data - BBOA1GET
- Invoke - BBOA1INV
- Host Service - BBOA1SRV
- JCA Adapter APIs

## Register

Using the BBOA1REG API, you can register with a local Liberty server. The BBOA1REG API requests that a group of optimized connections to a local Liberty server be allocated and registered under the specified register name.

*Table 145. BBOA1REG API syntax*

API	Syntax
BBOA1REG	BBOA1REG (wologroupnamepart1, wologroupnamepart2, wologroupnamepart3, registername, minconn, maxconn, registerflags, rc, rsn)

The BBOA1REG API accepts the following input parameters:

### **wologroupnamepart1**

An entry variable or entry constant that contains the first part of the name of the optimized local adapter group to be joined. It must be a null-terminated string of exactly 8 characters, and it must be passed by reference.

### **wologroupnamepart2**

An entry variable or entry constant that contains the second part of the name of the optimized local adapter group to be joined. It must be a blank-padded string of exactly 8 characters, and it must be passed by reference.

### **wologroupnamepart3**

An entry variable or entry constant that contains the third part of the name of the optimized local adapter group to be joined. It must be a blank-padded string of exactly 8 characters, and it must be passed by reference.

### **registername**

An entry variable or entry constant that contains the name that is used to register a set of local connections. Later calls require this name to identify the pool of connections to use. It must be a blank-padded string of exactly 12 characters, and it cannot be used in the current address space.

### **minconn**

An integer that contains the initial minimum number of connections to allocate for this registration. The adapter attempts to reserve this number of connections with the associated server during registration.

**Important:** At minimum, one connection is allocated to bind with the target server even if the `minconn` parameter is specified as 0, so specifying 0 is the same as specifying 1.

#### **maxconn**

An integer that contains the maximum number of connections to allocate for this registration. The adapter attempts to extend the local connection pool up to this number during a Connection Get API request when the minimum number of connections are all in use.

#### **registerflags**

A 32-bit flag word that contains registration flags.

- **reg\_flag\_W2Cprop** - bit 31

The `reg_flag_W2Cprop` flag controls outbound transaction security propagation from the Liberty server to CICS.

- **reg\_flag\_C2Wprop** - bit 29

The `reg_flag_C2Wprop` flag propagates the identity on the calling task from CICS to the Liberty server. For transactions that are inbound from CICS, the flag controls how the identity is determined. When this bit is turned *on*, the CICS application task identity is used in the Liberty server authorization process. When this bit is turned *off*, the CICS region identity is used.

- **reg\_flag\_trcmod** - bit 0

Set the `reg_flag_trcmod` flag if you want to modify the optimized local adapter trace settings for the requested registration. If you do not set this flag, no change to the trace setting is made, and the system defaults or predefined trace settings that apply to the registration name or job name are used.

- **reg\_flag\_trcmore** - bit 1 and **reg\_flag\_trcsome** - bit 2

If you set `reg_flag_trcmod` flag to 1, you must also specify the level of tracing for the registration by setting the `reg_flag_trcmore` flag for detailed tracing or the `reg_flag_trcsome` flag for coarse-level tracing. If `reg_flag_trcmod` is set to 1, setting both the `reg_flag_trcmore` flag and the `reg_flag_trcsome` flag to 0 forces no tracing for the registration regardless of what pre-definitions or defaults are set.

The BBOA1REG API accepts the following output parameters:

**rc** An integer return code that indicates success or failure of this call.

#### **rsn**

An integer reason code that describes the reason for a failure on this call.

Usage notes:

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.
- The minimum connections requested is validated against the server maximum connections. A minimum connection (`minconn`) value of 3 means that three connections are reserved during the register call. If more than three connections are requested at a given time, the connection pool can increase to the maximum connection (`maxconn`) value. When the number of all connections to a server reaches the maximum that is permitted, all subsequent Connection Get API requests for that server are rejected, even if the `maxconn` value is not yet reached.

**Important:** Use caution in setting the minimum connections value. Except in specific instances, do not set a large value because resources in the Liberty server are reserved for each connection.

- Multiple calls to the Register API can be made under the same address space, thread, or Customer Information Control System (CICS) task; however, they cannot share the same register name. The register name must be a unique name.
- Use the Unregister API call to remove this registration and release the connection pool associated with it.

- When the address space that makes a register call terminates, the registration is automatically terminated and the connections are released.

Return and reason codes:

Table 146. BBOA1REG API return and reason codes

Return Code	Reason Code	Description	Action
0	-	Success	
4	8.5.5.2 <sup>4</sup>	The transactional register flag was set to 1 in an environment where the adapter does not support global transactions.	This setting is ignored and processing continues.
8	-	Error - see reason code	
	8	The registration name token already exists.	Unregister this name before you call the Register API.
	12	The specified minimum connections parameter is larger than the maximum.	Ensure that the minimum connections setting is less than, or equal to, the maximum setting.
	14	Out of shared memory while trying to create registration.	Increase the shared memory allocation for the optimized local adapter or issue unregister calls to reduce resource consumption.
	74	Input register name contains a null.	Before you call the Register API, pad the register name with blank spaces so that the name is exactly 12 characters long.
	8.5.5.9 236	WOLA name part 2 or 3 is empty or missing.	Ensure that WOLA name part 2 and 3 are specified on the BBOA1REG call.
	8.5.5.9 480	The client cannot become authorized to invoke the register function.	This condition is unexpected. Ensure that the target server is running and that the zosLocalAdapters service is configured in the server instance.
	8.5.5.9 481	The client could not find the authorized function table for zosLocalAdapters services.	Ensure that the zosLocalAdapters feature is configured on the target server instance.
12	10	The API could not locate the selected optimized local adapters group.	Ensure that the Liberty server and target server are started, verify that the optimized local adapters support is active, and try again.
	14	The user ID is not authorized for the requested Liberty server.	Ensure that the user ID is authorized to the CBIND SAF class for the requested Liberty server.
	16	Part 2 or part 3 of the optimized local adapters group name is not found.	Ensure that the optimized local adapter group name parameters that are being passed are valid and that the server is active.
	23	An error occurred while naming the token.	See the problem determination information on the WebSphere Application Server Support site.
	24	An error occurred while establishing the initial Liberty server local communication connection.	Refer to the Liberty server region logs for details on the local communication connect call.
	28	The registration identified with this name is not valid.	The specified register name is already registered, but the registration is missing. As a workaround, call the Unregister API and attempt to call the Register API again. If the problem continues, see the problem determination information on the WebSphere Application Server Support site.
	68	An attachment to shared memory failed.	See the problem determination information on the WebSphere Application Server Support site.
	86	The Liberty server master BGVT cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	8.5.5.9 232	An out of memory condition occurred during a register call.	Ensure that memory is available to the client in subpool 0. Try the BBOA1REG call again.
	8.5.5.9 234	The client could not bind to the Liberty server instance.	Ensure that the Liberty server instance started and that the zosLocalAdapters service is configured in the server instance.

Table 146. BBOA1REG API return and reason codes (continued)

Return Code	Reason Code	Description	Action
	8.5.5.9 238	The client could not locate the target server's registration.	This condition is unexpected. Ensure that the target server instance started and that the zosLocalAdapters feature is configured. If the server stopped, start it and try the BBOA1REG call again.

## Unregister

Unregister from the local optimized local adapter group and Liberty server using the BBOA1URG API.

*Table 147. BBOA1URG API syntax.* This API requests that a group of optimized connections to a local optimized local adapter group and Liberty server be released using the specified register name.

API	Syntax
BBOA1URG	BBOA1URG (registername, unregflags, rc, rsn)

The BBOA1URG API accepts the following input parameters:

### registername

An entry variable or entry constant that contains the name to use to unregister a set of local connections. The value must be exactly 12 characters, blank padded, and the same name that is used on the Register API call.

### unregisterflags

A 32-bit flag word that contains unregistration flags.

- **Reserved** - bit 0-30
- **Force (0|1)** - bit 31

Specify 1 to force the unregister request. By default, an unregister request is complete if all connections are returned to the connection pool. If all the connections are not returned to the pool, a warning is returned to the caller. The unregister process is complete when the last connection is returned to the pool. Make a second register request with the force bit set to 1 to force the unregister process to complete and invalidate all remaining connection handles for that registration.

The BBOA1URG API accepts the following output parameters:

**rc** An integer return code that indicates success or failure of this call.

### rsn

An integer reason code that describes the reason for a failure on this call.

Usage notes:

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.
- If the Unregister API is not called and the address space that made a register call terminates, an unregister call is done automatically and the connections are released.
- Any connection handles for this registration that are active when the unregister call occurs might continue to be valid until they are returned to the connection pool by using the Connection Release API. To force the connection handles to be cleaned up, a second unregister call must be made, specifying the force flag. This invalidates all outstanding connection handles.

Return and reason codes:

Table 148. BBOA1URG API return and reason codes

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Warning - see reason code	

Table 148. BBOA1URG API return and reason codes (continued)

Return Code	Reason Code	Description	Action
	66	The unregister call is delayed until all the connections are returned to the pool.	Unregistration completes when the last connection is returned to the free pool.
8	-	Error - see reason code	
	8	The registration token name does not exist.	You must register this name before calling the Unregister API for it.
	64	The <i>force</i> option cannot be specified until a normal unregister is issued.	Call the Unregister API without specifying the <i>force</i> option.
	82	An attempt to unregister this registration was already made.	Wait for the previous unregister request to complete or reissue this unregister with the <i>force</i> option.
	8.5.5.9 228	The unregister call could not complete because the registration has already been reused.	No action is required.
	8.5.5.9 230	The connection pool could not be cleaned up on an unregister force call.	No action is required. To avoid using an unregister force call, ensure that your application returns all of the connection handles back to the pool before calling unregister.
	8.5.5.9 480	The client could not become authorized to call the unregister function.	This condition is unexpected. Ensure that the target server is running and that the zosLocalAdapters service is configured in the server instance.
12	86	The Liberty server master BGVV cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Connection Get

This API requests that an available connection from the pool that was created with the selected registration name is returned.

Table 149. BBOA1CNG API syntax

API	Syntax
BBOA1CNG	BBOA1CNG (registername, connectionhandle, waittime, rc, rsn)

The BBOA1CNG API accepts the following input parameters:

### registername

An entry variable or entry constant that contains the name to be used to locate the connection pool from which to retrieve a connection. This must be a blank padded string of exactly 12 characters.

### connectionhandle

A 12-byte connection handle that must be passed on later requests for actions on this connection.

### waittime

An integer that contains the number of seconds to wait for the connection to complete before returning a connection unavailable reason code. A value of 0 implies there is no wait time and the API waits indefinitely. The *waittime* parameter applies only to the process of obtaining a WOLA connection from the connection pool. When the connection is obtained, it is used to receive a request from the server with an unlimited wait time.

The BBOA1CNG API accepts the following output parameters:

**rc** An integer return code that indicates success or failure of this call.

**rsn**

An integer reason code that describes the reason for a failure on this call.

Usage notes:

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.
- Ensure that a successful Register API call was completed in the current address space with a matching name before you use the Connection Get API.

Return and reason codes:

*Table 150. BBOA1CNG API return and reason codes*

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Warning - see reason code	
8	-	Error - see reason code	
	8	The registration name token does not exist.	Register this name before you call the name with the Connection Get API.
	10	The connection is unavailable. The wait time expired before the connection request could be obtained.	The application behavior varies. Wait and try again, or issue the abend macro to terminate the task that called the Connection Get API. You can also increase the maximum connections setting on the Register API call.
	24	After a successful register call, an error occurred when getting a connection from the pool.	Verify that the server is started. If it is not working, restart the server and try the API request again.
	28	The registration was found, but it is inactive.	
	8.5.5.9 224	An incomplete registration was found.	This condition is unexpected. Use the BBOA1URG service to unregister, and use the BBOA1REG service to register again.
	8.5.5.9 480	The client could not become authorized to call the get connection function.	This condition is unexpected. Ensure that the target server is running and that the zosLocalAdapters service is configured in the server instance.
	8.5.5.9 482	The client could not reconnect to the target server instance after the server was restarted.	This condition is unexpected. Use the BBOA1URG service to remove the registration, and use the BBOA1REG service to create a new one.
	8.5.5.9 483	The client could not reconnect to the target server instance after the server was restarted.	This condition is unexpected. Use the BBOA1URG service to remove the registration, and use the BBOA1REG service to create a new one.
12	10	The API could not locate the selected optimized local adapters group.	Ensure that the Liberty server and target server are started, verify that the optimized local adapters support is active, and try again.
	8.5.5.9 14	The user ID is not authorized for the requested Liberty server.	Ensure that the user ID is authorized to the CBIND SAF class for the requested Liberty server.
	86	The Liberty server master BGVT cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Connection Release

The Connection Release API requests that a connection is returned to the pool that it was retrieved from and is made available for another requester.

Table 151. BBOA1CNR API syntax

API	Syntax
BBOA1CNR	BBOA1CNR (connectionhandle, rc, rsn)

The BBOA1CNR API accepts the following input parameter:

### connectionhandle

A 12-byte connection handle that indicates the previously obtained connection that is to be released back into the connection pool.

The BBOA1CNR API accepts the following output parameters:

**rc** An integer return code that indicates success or failure of this call.

### rsn

An integer reason code that describes the reason for a failure on this call.

### Usage notes

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.
- Before you use the Connection Release API, ensure that a successful Register API call is completed in the current address space with a matching name, and a successful Connection Get API call is completed to obtain the connection that is now to be released.

Table 152. BBOA1CNR API return and reason codes

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Unable to locate the optimized local adapter group and Liberty server. Any resources that are related to this connection were cleared.	None
8	-	Error-see reason code	
	36	The connection state is not valid.	The connection handle that is used for this request is in the wrong state. Refer to the API documentation for the rules on connection states.
	38	The client connection handle is not valid.	The client connection handle that is used for this request is not valid. Refer to the API documentation for information about client connection handles.
12	86	The Liberty server master BGVT cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Send Request

These APIs send a request into the local Liberty server for processing.

Table 153. BBOA1SRQ API syntax

API	Syntax
BBOA1SRQ	BBOA1SRQ (connectionhandle, requesttype, request servicename, request servicename1, requestdata, requestdatalen, async(0 1), responsedatalen, rc, rsn)

The BBOA1SRQ API accepts the following input parameters:

### connectionhandle

A 12-byte connection handle that is to be used for this request.

### requesttype

An integer that contains the request type that indicates the type of work request to process. The only supported value is 1 for local EJB work requests.

### request servicename

An EBCDIC character string up to 256 bytes in length that contains the name of the service to invoke. This parameter specifies the JNDI name of the local business interface.

### request servicename1

An integer that contains the length of the service name to start or 0 (zero) if the service name is null terminated.

### requestdata

A 31-bit pointer to the address of the start of the request data to send.

### requestdatalen

A 32-bit unsigned value that contains the length of the data to send.

### async(0|1)

Set **async** to 1 to indicate that the caller wants control returned immediately, even though the response length might not yet be known. If you set **async** to 0, the current thread waits for the Liberty server to return the response, and the API returns the response length in the **responsedatalen** output parameter.

The BBOA1SRQ API accepts the following output parameters:

### responsedatalen

A 32-bit unsigned value that contains the length of the response. The caller can use this length to acquire storage before you call the Get Data API to copy the data in. When you set **async** to 1, indicating the caller wants control back immediately, the value is set to 0xFFFFFFFF if the response is not yet received.

**rc** An integer return code that indicates success or failure of this call.

### rsn

An integer reason code that describes the reason for a failure on this call.

Usage notes:

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.
- Ensure that a successful Register API call was completed in the current address space with a matching name before you use the Send Request API.

Return and reason codes:

Table 154. BBOA1SRQ API return and reason codes

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Warning - see reason code	
8	-	Error - see reason code	
	8	The register name token already exists.	Ensure that the register name passed is valid.
	16	The request service name length is not valid.	Correct the program and try again.
	18	The request length exceeds the system limits.	The message size is larger than the Liberty server size can support. Verify that the size is valid. If the size is valid, ensure that the Liberty server size is large enough to accommodate the message size.
	32	The API call request type is not valid.	The request type is not valid. Correct the program and try the call again.
	34	The target service is not found.	Ensure that the application that contains the target enterprise bean is installed and started in the target server for the Liberty server.
	36	The connection state is not valid.	The connection handle that is used for the request is in the wrong state. Refer to the API documentation for the rules on connection states.
	38	The client connection handle is not valid.	The client connection handle that is used for the request is not valid. Refer to the API documentation for information about client connection handles.
	40	A local communication error occurred.	Check the Liberty server log for any local communication error messages.
	44	An exception or unexpected condition occurred in the target enterprise bean.	Refer to the Liberty server logs to review the exception data.
	46	An error occurred in the local communication send request call.	Check the Liberty server logs to determine the error.
	98	The beginning of the supplied request buffer cannot be accessed.	Ensure that the supplied request buffer address and length are correct.
	100	The end of the supplied request buffer cannot be accessed.	Ensure that the supplied request buffer address and length are correct.
12	10	The API could not locate the selected optimized local adapters group.	Ensure that the Liberty server and target server are started, verify that the optimized local adapters support is active, and try again.
	86	The Liberty server master BGVV cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Send Response

This API sends a response to a request back to the local Liberty server.

Table 155. BBOA1SRP API syntax

API	Syntax
BBOA1SRP	BBOA1SRP (connectionhandle, responsedata, responsedatalen, rc, rsn)

The BBOA1SRP API accepts the following input parameters:

**connectionhandle**

A 12-byte connection handle that is to be used for this response.

**responsedata**

A 31-bit pointer to the address of the start of the response data to send.

**requestdatalen**

A 32-bit unsigned value that contains the length of the data to send.

The BBOA1SRP API accepts the following output parameters:

**rc** An integer return code that indicates success or failure of this call.

**rsn**

An integer reason code that describes the reason for a failure on this call.

## Usage notes:

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.
- Ensure that a successful Register API call was completed in the current address space with a matching name before you use the Send Response API.
- Ensure that a successful Connection Get API call completed and the handle is provided as input on this call.
- Ensure that a successful receive Request Any, Receive Request Specific, or Host API call was issued and returned with request data for the connection handle. The connection must be in a state where the Send Response API is valid.

## Return and reason codes:

*Table 156. BBOA1SRP API return and reason codes*

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Warning - see reason code	
8	-	Error - see reason code	
	8	The register name token already exists.	Ensure that the register name passed is valid.
	18	The request length exceeds the system limits.	The message size is larger than the Liberty server size can support. Verify that the size is valid. If the size is valid, ensure that the Liberty server size is large enough to accommodate the message size.
	34	The target service is not found.	Ensure that the application that contains the target enterprise bean is installed and started in the target server for the Liberty server.
	36	The connection state is not valid.	The connection handle that is used for the request is in the wrong state. Refer to the API documentation for the rules on connection states.
	38	The client connection handle is not valid.	The client connection handle that is used for the request is not valid. Refer to the API documentation for information about client connection handles.
	40	A local communication error occurred.	Check the Liberty server log for any local communication error messages.
	46	An error occurred in the local communication send request call.	Check the Liberty server logs to determine the error.
	102	The beginning of the supplied response buffer cannot be accessed.	Ensure that the supplied response buffer address and length are correct.
	104	The end of the supplied response buffer cannot be accessed.	Ensure that the supplied response buffer address and length are correct.
	8.5.5.9 480	The client could not become authorized to call the send response function.	This condition is unexpected. Ensure that the target server is running and that the <code>zosLocalAdapters</code> service is configured in the server instance.

Table 156. BBOA1SRP API return and reason codes (continued)

Return Code	Reason Code	Description	Action
12	10	The API could not locate the selected optimized local adapters group.	Ensure that the Liberty server and target server are started, verify that the optimized local adapters support is active, and try again.
	86	The Liberty server master BGVV cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Send Response Exception

This API sends a ResourceException exception that contains response data back to the JCA caller in the local Liberty server.

Table 157. BBOA1SRX API syntax

API	Syntax
BBOA1SRX	BBOA1SRX (connectionhandle, excrespondata, excrespondatalen, rc, rsn)

The BBOA1SRX API accepts the following input parameters:

### connectionhandle

A 12-byte connection handle that is to be used for this response.

### excrespondata

A 31-bit pointer to the address of the start of the exception response data to send.

### excrespondatalen

A 32-bit unsigned value that contains the length of the exception response data to send. Exception response data is an EBCDIC string that describes the error.

The BBOA1SRX API accepts the following output parameters:

**rc** An integer return code that indicates success or failure of this call.

### rsn

An integer reason code that describes the reason for a failure on this call.

Usage notes:

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.
- Ensure that a successful Register API call completed in the current address space with a matching name before you use the send response call.
- Ensure that a successful Connection Get API call completed, and provide the handle as input on this API call.
- Ensure that a successful Receive Request Any, Receive Request Specific, or Host Service API call was issued and returned with request data for the connection handle. The connection must be in a state where the Send Response and Send Response Exception APIs are valid.

Return and reason codes:

Table 158. BBOA1SRX API return and reason codes

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Warning - see reason code	
8	-	Error - see reason code	
	8	The register name token already exists.	Ensure that the register name passed is valid.
	10	The connection handle is in a released or not valid state.	Ensure that a valid connection handle was passed.
	16	One or more parameters are not valid.	Verify that all the parameters are valid and try the call again.
	18	The request length exceeds the system limits.	The message size is larger than the Liberty server size can support. Verify that the size is valid. If the size is valid, ensure that the Liberty server size is large enough to accommodate the message size.
	36	The connection state is not valid.	The connection handle used for this request is in the wrong state. Refer to the API documentation for the rules on connection states.
	38	The client connection handle is not valid.	The client connection handle used for this request is not valid. Refer to the API documentation for information about client connection handles.
	40	A local communication error occurred.	Check the Liberty server log for any local communication error messages.
	46	An error occurred in the local communication send request call.	Check the Liberty server logs to determine the error.
	102	The beginning of the supplied response buffer cannot be accessed.	Ensure that the supplied response buffer address and length are correct.
	104	The end of the supplied response buffer cannot be accessed.	Ensure that the supplied response buffer address and length are correct.
	8.5.5.9 480	The client could not become authorized to call the send exception function.	This condition is unexpected. Ensure that the target server is running and that the zosLocalAdapters service is configured in the server instance.
12	10	The API could not locate the selected optimized local adapters group.	Ensure that the Liberty server and target server are started, verify that the optimized local adapters support is active, and try again.
	86	The Liberty server master BGVt cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Receive Request Any

This API receives a request and related data from a local Liberty server on any connection in the pool for the passed register name. The API returns request data length and a connection handle as output parameters. Calling the Get Data API with the returned connection handle returns the received message data.

Table 159. BBOA1RCA API syntax

API	Syntax
BBOA1RCA	BBOA1RCA (registername, connectionhandle, requestservername, requestservername1, requestdatalen, waittime, rc, rsn)

The BBOA1RCA API accepts the following input parameters:

**registername**

An entry variable or entry constant that contains the name to be used to locate the connection pool from which to retrieve a connection. The value must be a blank padded string of exactly 12 characters.

**waittime**

An integer that contains the number of seconds to wait for the connection to complete before it returns a connection unavailable reason code. A value of 0 indicates that there is no wait time and that the API waits indefinitely. The `waittime` parameter applies only to the process of obtaining a WOLA connection from the connection pool. When the connection is obtained, it is used to receive a request from the server with an unlimited wait time.

The BBOA1RCA API accepts the following input or output parameters:

**requestservicename**

An EBCDIC character string up to 256 bytes that contains the name of the service. This parameter is the name of the target service that is specified on the `InteractionSpec` interface by the Liberty server application. A value of \* indicates a receive request for all service names that arrive under the current register name.

**requestservicename1**

An integer that contains the length of the service name to start or 0 if the service name is null terminated.

The BBOA1RCA API accepts the following output parameters:

**connectionhandle**

A 12-byte connection handle that is returned and must be passed on later requests for actions on this connection.

**requestdatalen**

A 32-bit unsigned value is returned with the length of the data to receive.

**rc** An integer return code that indicates success or failure of this call.

**rsn**

An integer reason code that describes the reason for a failure on this call.

Usage notes:

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.
- Ensure that a successful Register API call was completed in the current address space with a matching name before you use this API.

Return and reason codes:

*Table 160. BBOA1RCA API return and reason codes*

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Warning - see reason code	
8	-	Error - see reason code	
	8	The register name token already exists.	Ensure that the register name passed is valid.
	10	The connection is unavailable. The wait time expired before the connection request could be obtained.	The application behavior varies. Wait and try again, or issue the <code>abend</code> macro to terminate the task that called the Connection Get API. You can also increase the maximum connections setting on the Register API call.

Table 160. BBOA1RCA API return and reason codes (continued)

Return Code	Reason Code	Description	Action
	16	The request service name length is not valid.	Correct the program and try the call again.
	19	A call to a local communication service received a non-zero return code.	
	21	A call to a local communication service received a non-zero return code.	
	38	The client connection handle is not valid.	The client connection handle used for this request was determined to be not valid. Refer to the API documentation for information about client connection handles.
	40	A local communication error occurred.	Check the Liberty server log for any local communication error messages.
	46	An error occurred in the local communication send request call.	Check the Liberty server logs to determine the error.
	8.5.5.9 224	An incomplete registration was found.	This condition is unexpected. Use the BBOA1URG service to unregister, and use the BBOA1REG service to register again.
	8.5.5.9 226	An incomplete connection handle was found.	This condition is unexpected. Use the BBOA1RCA service to try the request again.
	8.5.5.9 480	The client could not become authorized to call the receive request function.	This condition is unexpected. Ensure that the target server is running and that the zosLocalAdapters service is configured in the server instance.
	8.5.5.9 482	The client could not reconnect to the target server instance after the server was restarted.	This condition is unexpected. Use the BBOA1URG service to remove the registration, and use the BBOA1REG service to create a new one.
	8.5.5.9 483	The client could not reconnect to the target server instance after the server was restarted.	This condition is unexpected. Use the BBOA1URG service to remove the registration, and use the BBOA1REG service to create a new one.
12	10	The API could not locate the selected optimized local adapters group.	Ensure that the Liberty server and target server are started, verify that the optimized local adapters support is active, and try again.
	8.5.5.9 14	The user ID is not authorized for the requested Liberty server.	Ensure that the user ID is authorized to the CBIND SAF class for the requested Liberty server.
	24	After a successful registration call, an error occurred when getting a connection from the pool.	Verify that the server is started. If the server is not started, restart the server and try the API request again.
	86	The Liberty server master BGVTT cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Receive Request Specific

This API receives a request and related data from a local Liberty server for the specified connection handle. The API returns request data length as an output parameter. Calling the Get Data API with the specified connection handle returns the received message data.

Table 161. BBOA1RCS APIs syntax

API	Syntax
BBOA1RCS	BBOA1RCS (connectionhandle, requestservername, requestservername1, requestdatalen, async(0 1), rc, rsn)

The BBOA1RCS API accepts the following input parameters:

**connectionhandle**

A 12-byte connection handle that is to be used for the receive request.

**async(0|1)**

Set **async** to 1 to indicate that the caller wants control returned immediately, even though the response length might not yet be known. If you set **async** to 0, this call waits to receive a request from the Liberty server.

The BBOA1RCS API accepts the following input or output parameters:

**requestservername**

An EBCDIC character string up to 256 bytes that contains the name of the service. This parameter is the name of the target service that is specified on the InteractionSpec interface by the Liberty server application. A value of \* indicates that set up as a server for all service names that arrive under the current register name.

**requestservername1**

An integer that contains the length of the service name to start or 0 if the service name is null terminated.

The BBOA1RCS API accepts the following output parameters:

**requestdatalen**

A 32-bit unsigned value is returned that contains the length of the request data received. The caller can then use this length to acquire storage before you call the Get Data API to copy the data in. When **async** is set to 1, indicating the caller wants control back immediately, the value is set to 0xFFFFFFFF if the request data is not yet received. In this case, you must call the API again to retrieve an inbound request.

**rc** An integer return code that indicates success or failure of this call.

**rsn**

An integer reason code that describes the reason for a failure on this call.

Usage notes:

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.
- Ensure that a successful Register API call was completed in the current address space with a matching name before you use this API.

Return and reason codes:

Table 162. BBOA1RCS API return and reason codes

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Warning - see reason code	
8	-	Error - see reason code	
	8	The register name token already exists.	Ensure that the register name passed is valid.
	10	The connection handle is in a released state improper state.	Ensure that a valid connection handle passed.

Table 162. BBOA1RCS API return and reason codes (continued)

Return Code	Reason Code	Description	Action
	16	The request service name length is not valid.	Correct the program and try the call again.
	19	A call to a local communication service received a non-zero return code.	
	21	A call to a local communication service received a non-zero return code.	
	36	The connection state is not valid.	The connection handle used for this request is in the wrong state. Refer to the API documentation for the rules on connection states.
	38	The client connection handle is not valid.	The client connection handle used for this request is not valid. Refer to the API documentation for information about client connection handles.
	40	A local communication error occurred.	Check the Liberty server log for any local communication error messages.
	46	An error occurred in the local communication send request call.	Check the Liberty server logs to determine the error.
	76	An attempt to communicate with the server failed because the server is no longer running.	Start the server and try the communication again.
	78	An internal error occurred that caused the connection to select a request that was not a part of the transaction being processed by this connection.	Return the connection to the connection pool. If the problem continues, see the problem determination information on the WebSphere Application Server Support site.
	80	The transaction that is active on this connection timed out and the connection state cannot be reset so that another request is processed.	Return the connection to the connection pool. If the problem continues, see the problem determination information on the WebSphere Application Server Support site.
	8.5.5.9 226	An incomplete connection handle was found.	This condition is unexpected. Use the BBOA1CNR service to release the connection, and use the BBOA1CNG service to obtain a new connection.
	8.5.5.9 480	The client could not become authorized to call the receive request function.	This condition is unexpected. Ensure that the target server is running and that the zosLocalAdapters service is configured in the server instance.
12	10	The API could not locate the selected optimized local adapters group.	Ensure that the Liberty server and target server are started, verify that the optimized local adapters support is active, and try again.
	86	The Liberty server master BGVV cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Receive Response Length

The receive response length API retrieves the length of the response data from a prior send request call.

Table 163. BBOA1RCL API syntax

API	Syntax
BBOA1RCL	BBOA1RCL (connectionhandle, async(0 1), responsedatalen, rc, rsn)

The BBOA1RCL API accepts the following input parameters:

**connectionhandle**

A 12-byte connection handle that is to be used for this request.

**async(0|1)**

Set **async** to 1 to indicate that the caller wants control returned immediately, even though the response length might not be known. If you set **async** to 0, this call waits for the Liberty server to return the response, and the API returns the response length in the **responsedatalen** parameter.

The BBOA1RCL API accepts the following output parameters:

**requestdatalen**

A 32-bit unsigned value with the length of the received data is returned. The caller can use this length to acquire storage before you call the Get Data API to copy the data in. If you set **async** to 1, the value is set to 0xFFFFFFFF if the response data is not yet received.

**rc** An integer return code that indicates success or failure of this call.

**rsn**

An integer reason code that describes the reason for a failure on this call.

Usage notes:

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.
- Ensure that a successful Register API call was completed in the current address space with a matching name before you use this API.
- Ensure that a successful Connection Get API call completed and the handle is provided as input on this call.
- Ensure that a successful Send Request API call was completed before you make this call.

Return and reason codes:

*Table 164. BBOA1RCL API return and reason codes*

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Warning - see reason code	
8	-	Error - see reason code	
	8	The register name token already exists.	Ensure that the register name passed is valid.
	19	A call to a local communication service received a non-zero return code.	
	21	A call to a local communication service received a non-zero return code.	
	36	The connection state is not valid.	The connection handle used for this request was determined to be in the wrong state. Refer to the API documentation for the rules on connection states.
	38	The client connection handle is not valid.	The client connection handle used for this request was determined to be not valid. Refer to the API documentation for information about client connection handles.
	40	A local communication error occurred.	Check the Liberty server log for any local communication error messages.
	8.5.5.9 226	An incomplete connection handle was found.	This condition is unexpected. Use the BBOA1CNR service to release the connection, and use the BBOA1CNG service to obtain a new connection.
	8.5.5.9 480	The client could not become authorized to call the receive length function.	This condition is unexpected. Ensure that the target server is running and that the zosLocalAdapters service is configured in the server instance.

Table 164. BBOA1RCL API return and reason codes (continued)

Return Code	Reason Code	Description	Action
12	10	The API could not locate the selected optimized local adapters group.	Ensure that the Liberty server and target server are started, verify that the optimized local adapters support is active, and try again.
	86	The Liberty server master BGVT cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Get Message Data

This API copies the received message data. When this API call returns, the message is removed from the adapter message cache.

Table 165. BBOA1GET API syntax

API	Syntax
BBOA1GET	BBOA1GET (connectionhandle, msgdata, msgdatalen, rc, rsn, rv)

The BBOA1GET API accepts the following input parameters:

### connectionhandle

A 12-byte connection handle that is to be used for this request.

### msgdata

A 31-bit pointer to the address of the start of the data area to copy into. The storage that this parameter points to must be in a key that the caller can write in.

### msgdatalen

A 32-bit unsigned value that contains the length of the data to copy.

The BBOA1GET API accepts the following output parameters:

**rc** An integer return code that indicates success or failure of this call.

### rsn

An integer reason code that describes the reason for a failure on this call.

**rv** A 32-bit integer return value that contains the size of the context buffer for this request.

Usage notes:

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.
- Ensure that a successful Register API call was completed in the current address space with a matching name before you use the Send Request API.
- Ensure that a successful Connection Get API call completed and the handle is provided as input on this call.
- If the API caller input **msgdatalen** parameter is larger than the actual message response, the return code contains a 0 and the actual message length is provided to the return value.
-

**Important:** After the get message data call returns to the caller, the message data does not persist and the connection is returned to a state where it can be used for another send or receive request call. A subsequent call to get message data or receive response length is returned in error.

Return and reason codes:

*Table 166. BBOA1GET API return and reason codes*

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Warning - see reason code	
8	-	Error - see reason code	
	8	The register name token already exists.	Ensure that the register name passed is valid.
	36	The connection state is not valid.	The connection handle used for this request was determined to be in the wrong state. Refer to the API documentation for the rules on connection states.
	38	The client connection handle is not valid.	The client connection handle used for this request was determined to be not valid. Refer to the API documentation for information about client connection handles.
	40	A local communication error occurred.	Check the Liberty server log for any local communication error messages.
	48	An error occurred in the local communication read request.	Check the Liberty server logs to determine the error.
	72	Response length input parameter is not large enough to contain the response message.	Only a portion of the message is returned. The remainder is discarded. Refer to the return value for the size of the message response.
	98	The beginning of the supplied request buffer cannot be accessed.	Ensure that the supplied request buffer address and length are correct.
	100	The end of the supplied request buffer cannot be accessed.	Ensure that the supplied request buffer address and length are correct.
	102	The beginning of the supplied response buffer cannot be accessed.	Ensure that the supplied response buffer address and length are correct.
	104	The end of the supplied response buffer cannot be accessed.	Ensure that the supplied response buffer address and length are correct.
	8.5.5.9 226	An incomplete connection handle was found.	This condition is unexpected. Use the BBOA1CNR service to release the connection, and use the BBOA1CNG service to obtain a new connection.
	8.5.5.9 480	The client could not become authorized to call the get data function.	This condition is unexpected. Ensure that the target server is running and that the zosLocalAdapters service is configured in the server instance.
12	10	The API could not locate the selected optimized local adapters group.	Ensure that the Liberty server and target server are started, verify that the optimized local adapters support is active, and try again.
	86	The Liberty server master BGVT cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Invoke

This API uses other underlying primitive API functions to call a method in a local Liberty server. It is designed to be used in situations where the response output area maximum size is known in advance.

Table 167. BBOA1INV API syntax

API	Syntax
BBOA1INV	BBOA1INV (registername, requesttype, request servicename, request servicename1, requestdata, requestdatalen, responsedata, responsedatalen, waittime, rc, rsn, rv)

The BBOA1INV API accepts the following input parameters:

### **registername**

An entry variable or entry constant that contains the name to be used to locate the connection pool to retrieve a connection for this invocation. The value must be a blank padded string of exactly 12 characters.

### **requesttype**

An integer that contains the request type, which indicates the type of work request to process. The only supported value is 1 for local EJB work requests.

### **request servicename**

An EBCDIC character string up to 256 bytes in length that contains the name of the service to invoke. This parameter specifies the JNDI name of the local business interface.

### **request servicename1**

An integer that contains the length of the service name to start or 0 if the service name is null terminated.

### **requestdata**

A 31-bit pointer to the address of the start of the request data to send.

### **requestdatalen**

A 32-bit unsigned value that contains the length of the request data to send.

### **responsedata**

A 31-bit pointer to the address of the start of the response data area to copy into. The storage this parameter points to must be in a key that the caller can write in.

### **responsedatalen**

A 32-bit unsigned value that contains the length of the response data to send.

### **waittime**

An integer that contains the number of seconds to wait for the connection to complete before it returns a connection unavailable reason code. A value of 0 (zero) indicates that there is no timeout and that this API waits indefinitely. The waittime parameter applies only to the process of obtaining a WOLA connection from the connection pool. When the connection is obtained, it is used to receive a request from the server with an unlimited wait time.

The BBOA1INV API accepts the following output parameters:

**rc** An integer return code that indicates success or failure of this call.

### **rsn**

An integer reason code that describes the reason for a failure on this call.

**rv** A 32-bit integer return value that contains the size of the message data that was received and copied into the caller response area.

Usage notes:

- Ensure that the Liberty server that you specified on this call is started and the support for local adapters is enabled.

- Ensure that a successful Register API call was completed in the current address space with a matching name before you use the Send Request API.
- If the API caller input **responseDataLen** parameter is larger than the actual message response, the return code contains a 0 (zero) and the actual message length is provided in the return value.

Return and reason codes:

*Table 168. BBOA1INV API return and reason codes*

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Warning - see reason code	
8	-	Error - see reason code	
	8	The register name token does not exist.	Ensure that the register name passed is valid.
	10	The connection is unavailable. The wait time expired before the connection request is obtained.	The application behavior varies. Wait and retry, or accept this failed Invoke API call. Another option is to increase the maximum connections setting on the Register API call.
	16	The request service name length is not valid.	Correct the program and try the call again.
	18	The response length exceeded the system limits.	The message size is larger than the Liberty server size can support. Verify that the size is valid. If the size is valid, ensure that the Liberty server size is large enough to accommodate the message size.
	19	A call to a local communication service received a non-zero return code.	
	21	A call to a local communication service received a non-zero return code.	
	24	After a successful register call, an error occurred when getting a connection from the pool.	Verify that the server is started. If it is not working, restart the server and try the API request again.
	26	The global transaction cannot begin.	
	28	The registration was found, but it is inactive.	
	32	The request type on the API call is not valid.	The request type parameter is not valid. Correct the program and try the call again.
	34	The target service not found.	Ensure the application that contains the target enterprise bean is installed and started in the target Liberty server.
	36	The connection state is not valid.	The connection handle used for this request was determined to be in the wrong state. Refer to the API documentation for the rules on connection states.
	38	The client connection handle is not valid.	The client connection handle used for this request was determined to be not valid. Refer to the API documentation for information about client connection handles.
	40	A local communication error occurred.	Check the Liberty server log for any local communication error messages.
	44	An exception or unexpected condition occurred in the target enterprise bean.	Refer to the Liberty server logs to review the exception data.
	46	An error occurred in the local communication send request.	Refer to the Liberty server logs to determine the error.
	48	An error occurred in the local communication read request.	Check the Liberty server logs to determine the error.
	72	Response length input parameter is not large enough to contain the response message.	Only a portion of the message is returned. The remainder is discarded. Refer to the return value for the size of the message response.

Table 168. BBOA1INV API return and reason codes (continued)

Return Code	Reason Code	Description	Action
	98	The beginning of the supplied request buffer could not be accessed.	Ensure that the supplied request buffer address and length are correct.
	100	The end of the supplied request buffer could not be accessed.	Ensure that the supplied request buffer address and length are correct.
	102	The beginning of the supplied response buffer could not be accessed.	Ensure that the supplied response buffer address and length are correct.
	104	The end of the supplied response buffer could not be accessed.	Ensure that the supplied response buffer address and length are correct.
	8.5.5.9 224	An incomplete registration was found.	This condition is unexpected. Use the BBOA1URG service to unregister, and use BBOA1REG to register again.
	8.5.5.9 226	An incomplete connection handle was found.	This condition is unexpected. Use the BBOA1INV service to try the request again.
	8.5.5.9 480	The client could not be authorized to call the invoke function.	This condition is unexpected. Ensure that the target server is running and that the zosLocalAdapters service is configured in the server instance.
	8.5.5.9 482	The client was not able to reconnect to the target server instance after the server was restarted.	This condition is unexpected. Use the BBOA1URG service to remove the registration, and use the BBOA1REG service to create a new one.
	8.5.5.9 483	The client was not able to reconnect to the target server instance after the server was restarted.	This condition is unexpected. Use the BBOA1URG service to remove the registration, and use the BBOA1REG service to create a new one.
12	10	The API could not locate the selected optimized local adapters group.	Ensure that the Liberty server and target server are started, verify that the optimized local adapters support is active, and try again.
	8.5.5.9 14	The user ID is not authorized for the requested Liberty server.	Ensure that the user ID is authorized to the CBIND SAF class for the requested Liberty server.
	24	After a successful register call, an error occurred while getting a connection from the connection pool.	Verify that the server is started. If it is not started, restart the server and try the API request again.
	86	The Liberty server master BGVT cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Host Service

The Host Service API uses other underlying primitive API functions to set up a native language z/OS program as a server and target for optimized local adapter calls from a local Liberty server. Use the API when you know the request area maximum size before you call the API.

Table 169. BBOA1SRV API syntax

API	Syntax
BBOA1SRV	BBOA1SRV (registername, requestservername, requestservername1, requestdata, requestdatalen, connectionhandle, waittime, rc, rsn, rv)

The BBOA1SRV API accepts the following input parameters:

**registername**

An entry variable or entry constant that contains the name to be used to locate the connection pool to retrieve a connection from for this call. The value must be a blank-padded string of exactly 12 characters.

**requestdata**

A 31-bit pointer to the address of the start of the request data received. The storage that this parameter points to must be in a key that the caller can write in.

**requestdatalen**

A 32-bit unsigned value that contains the length of the data area into which the message is received.

**connectionhandle**

A 12-byte connection handle that is returned to the caller and used for sending a response for this request.

**waittime**

An integer that contains the number of seconds to wait for the connection to complete before it returns a connection unavailable reason code. A value of 0 (zero) implies that there is no timeout, and the API waits indefinitely. The `waittime` parameter applies only to the process of obtaining a WOLA connection from the connection pool. When the connection is obtained, it is used to receive a request from the server with an unlimited wait time.

The BBOA1SRV API accepts the following input or output parameters:

**request servicename**

An EBCDIC character string up to 256 bytes that contains the name of the service. This parameter is the name of the target service that is specified on the InteractionSpec interface by the Liberty server application. A value of \* indicates set up as a server for all service names that arrive under the current register name.

**request servicename1**

An integer that contains the length of the service name to start or 0 if the service name is null terminated.

The BBOA1SRV API accepts the following output parameters:

**rc** An integer return code that indicates success or failure of this call.

**rsn**

An integer reason code that describes the reason for a failure on this call.

**rv** A 32-bit integer return value that contains the size of the message data that was received and copied into the caller response area.

Usage notes:

- Ensure that the Liberty server that you specified on this call are started and the support for local adapters is enabled.
- Ensure that a successful Register API call was completed in the current address space with a matching name before you use this API.
- If the API caller input **requestdatalen** parameter is larger than the actual message response, the return code contains a 0 (zero) and the actual message length is provided in the return value.
- The returned connection handle must be supplied on any response for this Host Service call using the Send Response API.

Return and reason codes:

Table 170. BBOA1SRV API return and reason codes

Return Code	Reason Code	Description	Action
0	-	Success	
4	-	Warning - see reason code	
8	-	Error - see reason code	
	8	The register name token already exists.	Ensure that the register name passed is valid.
	10	The connection handle is in a released state.	Ensure that a correct connection handle is passed.
	12	The connection handle is not in the connection that is in the registration name.	Correct to program and try the call again.
	16	The request service name length is not valid.	Correct the program and try the call again.
	18	The response length exceeded the system limits.	The message size is larger than the Liberty server size can support. Verify that the size is valid. If the size is valid, ensure that the Liberty server size is large enough to accommodate the message size.
	40	A local communication error occurred.	Check the Liberty server log for any local communication error messages.
	46	An error occurred in the local communication send request.	Refer to the Liberty server logs to determine the error.
	48	An error occurred in the local communication read request.	Check the Liberty server logs to determine the error.
	72	Response length input parameter is not large enough to contain the response message.	Only a portion of the message is returned. The remainder is discarded. Refer to the return value for the size of the message response.
	98	The beginning of the supplied request buffer cannot be accessed.	Ensure that the supplied request buffer address and length are correct.
	100	The end of the supplied request buffer cannot be accessed.	Ensure that the supplied request buffer address and length are correct.
	8.5.5.9 224	An incomplete registration was found.	This condition is unexpected. Use the BBOA1URG service to unregister, and use BBOA1REG service to register again.
	8.5.5.9 226	An incomplete connection handle was found.	This condition is unexpected. Use the BBOA1SRV service to try the request again.
	8.5.5.9 480	The client could not become authorized to call the host function.	This condition is unexpected. Ensure that the target server is running and that the zosLocalAdapters service is configured in the server instance.
	8.5.5.9 482	The client was not able to reconnect to the target server instance after the server was restarted.	This condition is unexpected. Use the BBOA1URG service to remove the registration, and use the BBOA1REG service to create a new one.
	8.5.5.9 483	The client was not able to reconnect to the target server instance after the server was restarted.	This condition is unexpected. Use the BBOA1URG service to remove the registration, and use the BBOA1REG service to create a new one.
12	10	The API could not locate the selected optimized local adapters group.	Ensure that the Liberty server and target server are started, verify that the optimized local adapters support is active, and try again.
	8.5.5.9 14	The user ID is not authorized for the requested Liberty server.	Ensure that the user ID is authorized to the CBIND SAF class for the requested Liberty server.
	86	The Liberty server master BGVV cannot be located.	The Liberty server was not started on the current z/OS operating system image. Ensure that the server is started before you start any optimized local adapters client processes.
	88	The Liberty server master client stub table cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.
	90	The master client stub table slot for the Liberty server optimized local adapters cannot be located.	A Liberty server was started on the current z/OS operating system image, but the server is not running at the level where the optimized local adapters client stub table is supported. Ensure that your application is running with the level of the optimized local adapters stubs that are compatible with the Liberty server on this z/OS system.

## Java EE Connector Architecture (JCA) adapters APIs

For calls from the Liberty server into a batch program or subsystem, the Liberty server application uses the standard JCA APIs. The following interfaces are customized for use with optimized local adapters:

- ConnectionSpec
- InteractionSpec
- Record I/O

### ConnectionSpec

Use the ConnectionSpec interface to pass connection-specific parameters when you obtain a connection from a connection factory. These parameters can override the parameters of the same name that are defined in the connection factory. For optimized local adapters, this interface is implemented as the `com.ibm.websphere.ola.ConnectionSpecImpl` class. The ConnectionSpecImpl class enables you to specify which optimized local adapters register name that you want to communicate with.

When you communicate with a CICS link server, the ConnectionSpecImpl class provides methods that you can use to override values that the link server uses. For example, you can specify the four-character transaction ID of the link server invocation transaction, BBO#. You can also specify whether to store request data in a CICS COMMAREA or CONTAINER object.

For information about methods in the ConnectionSpecImpl class, see the generated API documentation.

### InteractionSpec

Use the InteractionSpec interface to specify request-specific parameters to the resource adapter instance that you are connected to. For optimized local adapters, this interface is implemented as the `com.ibm.websphere.ola.InteractionSpecImpl` class. You can use the InteractionSpecImpl class to set the service name for the application to communicate with. The service name is hosted by the register name that was specified when the connection was obtained.

For information about methods in the InteractionSpecImpl class, see the generated API documentation.

### Record I/O

Use the Record interface to pass request and response data to the resource adapter instance that you are connected to. The optimized local adapters provide two implementations of the Record interface, IndexedRecord and MappedRecord. You can create both implementations by obtaining a reference to the RecordFactory from the JCA connection instance that the application uses.

Use an IndexedRecord object if you are passing data to a Batch or UNIX System Services program or if you are communicating with CICS using a COMMAREA or a single CONTAINER object. Add a byte array (`byte[]`) to the IndexedRecord object to represent the data that the program sends on the request. The response is also received into an IndexedRecord object. You can obtain the response data by retrieving the first entry from the IndexedRecord object and casting it to a byte array.

Use a MappedRecord object if you are passing data to CICS in multiple CONTAINER objects. The MappedRecord object contains name-value pairs, similar to what Map objects store. In the name-value pairs, the name is the name of the container that the data is transferred to, and the value is the actual data, specified as a byte array (`byte[]`). When you use a MappedRecord object to send a request, the response is also sent back using a MappedRecord object. The response contains the name of each container that contained response data and the associated data.

# Developing applications for use with z/OS Connect to reach z/OS assets



## IBM z/OS Connect overview



The IBM z/OS Connect offering is a Liberty feature that encapsulates calling z/OS target applications using REST (Representation State Transfer) calls.

z/OS Connect is designed to provide a fast, secure, reliable connector to reach any z/OS asset. z/OS Connect provides a standard way to identify these assets and reach the assets using REST technology. Where these assets run is specified in the z/OS Connect configuration, relieving clients applications in the cloud, mobile, and web worlds of the need to understand the details about how to reach them and how to convert payloads to and from the formats that the applications require.

### Benefits of using z/OS Connect

z/OS Connect adds value for z/OS customers by enabling users to consolidate multiple client connect pathways into a single common gateway or concentrator for synchronous calls to reach business assets and data on z/OS operating systems. Virtually any z/OS asset, applications and data, can be reached by using standard REST HTTP calls. This feature also provides the ability to inquire about, or discover, all assets that are defined in the z/OS Connect configuration repository. The following is a summary of the benefits of z/OS Connect:

- Provides RESTful access to identify and invoke z/OS-based business assets in CICS, IMS, UNIX System Services, and traditional batch environments, opening up these assets to cloud and mobile-based system of engagement environments.
- Functionality that is based on Liberty server technology, is lightweight and easily configurable, and provides z/OS differentiation with System Authorization Facility (SAF) security integration, z/OS Workload Manager (WLM), and Resource Recovery Services (RRS) integration. WLM integration means different URIs can have varying levels of priority and performance criteria.
- As a feature in the Liberty server on z/OS, you can integrate z/OS Connect with z/OS standard system management, which can run as a started task and integrate with z/OS automated operations.
- Provides the ability to secure individual or groups of z/OS Connect services with SAF security in which only specific users or groups can have access to specific services.
- Provides the ability to uniformly track requests from cloud, mobile, and web environments by using z/OS System Management Facility (SMF) services. This tracking means that z/OS customers can use their existing processes for auditing and chargeback for requests from these environments.
- Enables the ability to do an automatic conversion of the request payload from JavaScript Object Notation (JSON) form on input to binary form consumable by z/OS applications such as Cobol, PL/I, and C. The reverse for the response from the z/OS application, converting the output from binary to JSON form is also true.

### Using z/OS Connect REST APIs



z/OS<sup>®</sup> Connect provides a set of RESTful APIs that you can use to discover services, check service status, start or stop services, get statistics, and other operations.

### About this task

You can use z/OS Connect REST APIs from a client running in a web, mobile, or cloud environment.

## Procedure

1. Discover services in the z/OS Connect configuration.

Sample HTTP GET request:

```
https://host:port/zosConnect/services
```

Sample JSON payload returned:

```
{
  zosConnectServices: [
    {
      ServiceName: "recordOpsCreate"
      ServiceDescription: "Creates a new record"
      ServiceProvider: "SAMPLE-1.0"
      ServiceURL: "https://host:port/zosConnect/services/recordOpsCreate"
    },
    {
      ServiceName: "recordOpsDelete"
      ServiceDescription: "Deletes an existing record"
      ServiceProvider: "SAMPLE-1.0"
      ServiceURL: "https://host:port/zosConnect/services/recordOpsDelete"
    }
  ]
}
```

2. Retrieve configuration data for a service. Sample HTTP GET request:

```
https://host:port/zosConnect/services/recordOpsCreate
```

The output is returned in two parts: the first part contains the z/OS Connect configuration parameters and the second part has the configuration returned by the service provider implementation. The following is a sample of JSON payload that was returned:

```
{
  zosConnect: {
    serviceName: "recordOpsCreate"
    serviceDescription: "Creates a new record"
    serviceProvider: "SAMPLE-1.0"
    serviceURL: "https://host:port/zosConnect/services/recordOpsCreate"
    serviceInvokeURL: "https://host:port/zosConnect/services/recordOpsCreate?action=invoke"
    dataXformProvider: "jsonByte-1.0"
  },
  recordOpsCreate: {
    targetProgram: "CREATREC"
    timeout: "300ms"
  }
}
```

3. Retrieve service status. Sample HTTP GET request:

```
https://host:port/zosConnect/services/recordOpsCreate?action=status
```

Sample JSON payload returned.

```
{
  zosConnect:
  {
    serviceName: "recordOpsCreate"
    serviceDescription: "Creates a new record"
    serviceProvider: "SAMPLE-1.0"
    serviceURL: "https://host:port/zosConnect/services/recordOpsCreate"
    serviceInvokeURL: "https://host:port/zosConnect/services/recordOpsCreate?action=invoke"
    dataXformProvider: "jsonByte-1.0"
    serviceStatus: "Started"
  }
}
```

4. Retrieve request schema. Sample HTTP GET request:

```
https://host:port/zosConnect/services/recordOpsCreate?action=getRequestSchema
```

Sample JSON payload returned.

```
{
  <Request schema as returned by the data configured data transformer>
}
```

- Retrieve response schema. Sample HTTP GET request:

`https://host:port/zosConnect/services/recordOpsCreate?action=getResponseSchema`

Sample JSON payload returned.

```
{
  <Request schema as returned by the data configured data transformer>
}
```

- Retrieve statistics.

Statistics include z/OS Connect data for a service such as `InvokeRequestCount`, and a `TimeOfRegistrationWithZosConnect`, along with any other statistics returned by the service provider using the `getStatistics()` SPI implementation in the provider. Statistics for a particular service can be retrieved through a `/zosConnect/operation` or an `action=` request call. `/zosConnect/operations` requests offer more flexibility because the product can retrieve statistics for all services. If the authorization interceptor is enabled, then the product returns statistics for only those services that the user can request. See the documentation about z/OS Connect security for more details.

Sample HTTP GET request to return statistics using `action=getStatistics`:

`https://host:port/zosConnect/services/recordOpsCreate?action=getStatistics`

Sample JSON payload returned.

```
{
  recordOpsCreate:
  {
    ServiceProvider: "SAMPLE-1.0"
    InvokeRequestCount: 100
    TimeOfRegistrationWithZosConnect: "xxx-xx-xx xx:xx:xx:xxx xxx"
    ServiceStatistics:
    {
      <JSON name value pairs showing statistical information the service returned>
    }
  }
}
```

- Retrieving statistics for a service can be also accomplished using the `zosConnect/operations/getStatistics` REST API.

Information returned includes statistics for all services that the current user can request.

Sample HTTP GET request using `/zosConnect/operation/getStatistics` :

`https://host:port/zosConnect/operations/getStatistics`

Sample JSON payload returned.

```
{
  zosConnectStatistics:
  [
    {
      recordOpsCreate:
      {
        ServiceProvider: "SAMPLE-1.0"
        InvokeRequestCount: 100
        TimeOfRegistrationWithZosConnect: "xxx-xx-xx xx:xx:xx:xxx xxx"
        ServiceStatistics:
        {
          <JSON name value pairs showing statistical information the service returned>
        }
      }
    },
    {
      recordOpsDelete:
      {
        ServiceProvider: "SAMPLE-1.0"
        InvokeRequestCount: 100
      }
    }
  ]
}
```

```

        TimeOfRegistrationWithZosConnect: "xxx-xx-xx xx:xx:xx:xxx xxx"
    ServiceStatistics:
    {
    <JSON name value pairs showing statistical information the service returned>
    }
    }
}
]
}

```

If there are no services registered with z/OS Connect, the output resembles:

```

{
zosConnectStatistics:[]
}

```

- Retrieve statistics for all services that are defined for a specific service provider using the `zosConnect/operations/getStatistics` REST API.

Sample HTTP GET request:

```
https://host:port/zosConnect/operations/getStatistics?provider=SAMPLE-1.0
```

Sample format/output:

```

{
  recordOpsCreate:
  {
    ServiceProvider: "SAMPLE-1.0"
    InvokeRequestCount: 100
    TimeOfRegistrationWithZosConnect: "xxx-xx-xx xx:xx:xx:xxx xxx"
    ServiceStatistics:
    {
      .. JSON name value pairs showing statistical information the service returned.
    }
  }
}

```

- Retrieve statistics for a single service using the `zosConnect/operations/getStatistics?service=<service name>` REST API. This operation is equivalent to specifying `action=getStatistics` on a service.

HTTP GET request on:

```
https://host:port/zosConnect/operations/getStatistics?service=recordOpsCreate
```

Sample JSON payload returned:

```

{
  recordOpsCreate:
  {
    ServiceProvider: "SAMPLE-1.0"
    InvokeRequestCount: 100
    TimeOfRegistrationWithZosConnect: "xxx-xx-xx xx:xx:xx:xxx xxx"
    ServiceStatistics:
    {
      <JSON name value pairs showing statistical information the service returned>
    }
  }
}

```

- Stop z/OS Connect services by using an HTTP POST or PUT request with `action=stop`, or start the services by using HTTP POST or PUT with the `action=start` query string.  
Stop and start actions do not require a payload. If one is provided, it is ignored. A user can retrieve the status of a z/OS Connect service using HTTP GET on the service name with the `action=status` query string to retrieve the service status. If the authorization interceptor provided by z/OS Connect is enabled, the user that is requesting the status or state change must be in the operator or administrator group required for the service. For each, the Service Provider SPI is called by z/OS Connect to notify it that these actions have been requested. The method names that are in the SPI for this are `stop()`, `start()`, and `status()`.

**Note:** z/OS Connect does not persist any state that is related to the service and instead delegates this to the service provider.

The service provider can send responses other than stop or start. z/OS Connect allows for a custom status to be returned.

Stop a service sample using HTTP POST or PUT:

```
https://host:port/zosConnect/services/recordOpsCreate?action=stop
```

Sample JSON payload returned:

```
{
  zosConnect:
  {
    serviceName: "recordOpsCreate"
    serviceDescription: "Creates a new record"
    serviceProvider: "SAMPLE-1.0"
    serviceURL: "https://host:port/zosConnect/services/recordOpsCreate"
    serviceInvokeURL: "https://host:port/zosConnect/services/recordOpsCreate?action=invoke"
    dataXformProvider: "jsonByte-1.0"
    serviceStatus: "Stopped"
  }
}
```

11. Start a service sample using HTTP POST or PUT:

```
https://host:port/zosConnect/services/recordOpsCreate?action=start
```

Sample JSON payload returned:

```
{
  zosConnect:
  {
    serviceName: "recordOpsCreate"
    serviceDescription: "Creates a new record"
    serviceProvider: "SAMPLE-1.0"
    serviceURL: "https://host:port/zosConnect/services/recordOpsCreate"
    serviceInvokeURL: "https://host:port/zosConnect/services/recordOpsCreate?action=invoke"
    dataXformProvider: "jsonByte-1.0"
    serviceStatus: "Started"
  }
}
```

12. Invoke services using the z/OS Connect query string: `action=invoke`, which runs the `invoke()` method of the Service Provider SPI implementation.

The sample in this step runs the `invoke` method for the service named `recordOpsCreate` and passes a JSON object payload in the request body.

The z/OS Connect `invoke` method supports an input payload in JSON object form for this request. In the code example, it is assumed that z/OS Connect looked up the Service Provider and identified a service reference for the service called `SAMPLE-1.0`. There is also a data transformation reference in the z/OS Connect service definition with a provider called `jsonByte-1.0`. With this in place, when the `invoke` method of the service provider gets control and it calls the `getBytes()` method, the data transformation implementation gets control and converts the request payload from JSON to a byte array and returns it to the service provider.

If the URL that the `invoke` action request came in with contains query parameters, these parameters along with other HTTP request information are passed to the service provider using the `com.ibm.wsspi.zos.connect.HttpZosConnectRequest` SPI interface provided by z/OS Connect. Interceptors processed for actions or operations also receive HTTP request information through the same object.

Another invocation style that is supported by z/OS Connect provides a means to define a user-defined URI as the `invokeURI` in the z/OS Connect service definition. With this style, the HTTP request does not have to contain `zosConnect/services` and can instead be a user-defined string.

When this style is employed, z/OS Connect supports use of other HTTP methods, such as GET, PUT, POST, and DELETE. Requests arriving with this URI, regardless of the HTTP method employed, pass through z/OS Connect interceptors and are passed to the `invoke()` method of the service provider.

Sample using HTTP POST or PUT:

```
https://host:port/zosConnect/services/recordOpsCreate?action=invoke
{
<JSON object passed in for the service invocation>
}
```

Sample JSON payload returned:

```
{
<JSON object returned from the service invocation>
}
```

## Creating a z/OS Connect service provider



8.5.5.2

z/OS<sup>®</sup> Connect provides the `com.ibm.wsspi.zos.connect.Service` SPI that supports the creation of service providers that you can use to process requests arriving in to the z/OS Connect servlet.

### About this task

z/OS Connect service providers can be written and delivered by any component to plug into the framework. A WOLA service provider is included with z/OS Connect.

A service provider implemented for z/OS Connect is an OSGi service that connects and interacts with z/OS Connect through the OSGi framework.

### Procedure

1. Create a service provider that implements the z/OS Connect `com.ibm.wsspi.zos.connect.Service` SPI.
2. Edit the service metatype configuration so that it specifies the following attribute definition:

```
<AD id="com.ibm.ws.zos.connect.serviceType" required="false" type="String"ibm:final="true"name="internal"description="i
```

The `ibm:final` attribute indicates that the value cannot be specified in the configuration, and the `name="internal"` attribute indicates that tools do not display this property.

The Java™ API documentation for each Liberty SPI is available in a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

For more information, see the documentation on extending Liberty.

**Note:** The Java API documentation for each Liberty SPI is detailed in the Programming Interfaces (APIs) section of the documentation, and is also available as a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

## Creating a z/OS Connect service at run time

8.5.5.7

To process incoming requests, you can create a z/OS connect service at run time by using the `com.ibm.wsspi.zos.connect.ServiceController` service programming interface (SPI).

### About this task

You can dynamically create a z/OS Connect service provider at run time based on the configuration that is stored in an external repository.

### Procedure

1. Create a service provider that implements the z/OS Connect `com.ibm.wsspi.zos.connect.ServiceController` SPI.
2. At run time, register the service with the OSGi framework that is using the `theregisterService` method on the `BundleContext` attribute.

```
Dictionary<String, Object> dynamicServiceProps = new Hashtable<String, Object>();
dynamicServiceProps.put(ServiceControllerConstants.SERVICE_NAME, "myNewService");
dynamicServiceProps.put(ServiceControllerConstants.INVOKE_URI, new String[] { "/u/my/ur11",
"/u/myur12", "/u/my/ur13*" });
ServiceRegistration<ServiceController> dynamicServiceReg =
    bundleContext.registerService(com.ibm.wsspi.zos.connect.ServiceController.class, new
MyServiceController(), dynamicServiceProps);
```

**Important:** The Java API documentation for each Liberty SPI is detailed in the Programming Interfaces (APIs) section of the documentation, and is also available as a separate .zip file in one of the subdirectories of the `${wlp.install.dir}/dev` directory. For more information, see the documentation on extending Liberty.

## Creating a z/OS Connect interceptor



8.5.5.2

Use z/OS® Connect SPI to create interceptor `preInvoke` and `postInvoke` implementations that manage service requests such as `invoke`, `status`, `start`, and `stop`. Interceptors are OSGi services that implement the `com.ibm.wsspi.zos.connect.Interceptor` SPI provided by z/OS Connect.

### About this task

z/OS Connect includes several interceptors. The `com.ibm.wsspi.zos.connect.AuthorizationInterceptor` provides z/OS SAF and LDAP authorization checks z/OS Connect operations, such as `start`, `stop`, and `invoke`. The `com.ibm.wsspi.zos.connect.Audit` implementation, records z/OS SMF recording of request data on z/OS Connect operations.

You can use interceptors for various purposes. z/OS Connect has no visibility into uses of interceptors. For example, an interceptor might be written to do some infrastructure setup that is based on the message payload before the request is processed. z/OS Connect provides a copy of the input request payload to all interceptors.

An interceptor implemented for z/OS Connect is an OSGi service that connects and interacts with z/OS Connect through the OSGi framework.

### Procedure

1. The interceptor must implement the z/OS Connect `com.ibm.wsspi.zos.connect.Interceptor` SPI.
2. Edit the service metatype configuration so that it specifies following attribute definition:

```
<AD id="com.ibm.ws.zos.connect.interceptorType" required="false" type="String"ibm:final="true"name="internal"description
```

The `ibm:final` attribute indicates that the value cannot be specified in the configuration, and the `name="internal"` attribute indicates that tools do not display this property.

The Java™ API documentation for each Liberty SPI is available in a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

For more information, see the documentation on extending Liberty.

**Note:** The Java API documentation for each Liberty SPI is detailed in the Programming Interfaces (APIs) section of the documentation, and is also available as a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

## Creating a z/OS Connect data transformer



8.5.5.2

You can use the z/OS® Connect SPI to create a custom data transformer. Data transformers are OSGi services that implement the `com.ibm.wsspi.zos.connect.DataXform` SPI that is provided by z/OS Connect.

## About this task

z/OS Connect data transformers are written and delivered by any component to plug into the framework. A data transformer is included with z/OS Connect and provides both to and from JSON byte arrays that are consumable by COBOL, PL/I, and C programs on z/OS.

A data transformer that is implemented for z/OS Connect is an OSGi service that connects and interacts with z/OS Connect through the OSGi framework.

## Procedure

1. Implement the z/OS Connect `com.ibm.ws.zos.connect.DataXform` SPI in the service.
2. Edit the metatype configuration so that it specifies the following attribute definition:

```
<AD id="com.ibm.ws.zos.connect.dataXformType" required="false" type="String" ibm:final="true" name="internal" description="Data Xform Type" />
```

The `ibm:final` attribute indicates that the value cannot be specified in the configuration, and the `name="internal"` attribute indicates that tools do not display this property.

The Java™ API documentation for each Liberty SPI is available in a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

For more information, see the documentation on extending Liberty.

**Note:** The Java API documentation for each Liberty SPI is detailed in the Programming Interfaces (APIs) section of the documentation, and is also available as a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

## Conversion for z/OS Connect data transformation



8.5.5.2

The z/OS Connect feature runs in a WebSphere Application Server for z/OS, Liberty environment. You can use the BBGLS2JS and BBGJS2LS Job Control Language (JCL) tools to generate the necessary z/OS Connect artifacts to facilitate data conversion.

### BBGLS2JS: High-level language to binding and schema file conversion for z/OS Connect data transformation

The BBGLS2JS Job Control Language procedure generates a JavaScript Object Notation (JSON) schema and binding files from a high-level data structure. The files that are generated are used by the z/OS Connect data transformation process. It is based on DFHLS2JS from the Customer Information Control Center (CICS) Transaction Server Mobile Extensions feature pack.

See the documentation for usage information and examples on using the BBGLS2JS tool. Where the documentation refers to DFHLS2JS, use BBGLS2JS. [http://www-01.ibm.com/support/knowledgecenter/SSGMCP\\_5.1.0/com.ibm.cics.ts.mobileextensions.doc/reference/dfhws\\_ls2js.html](http://www-01.ibm.com/support/knowledgecenter/SSGMCP_5.1.0/com.ibm.cics.ts.mobileextensions.doc/reference/dfhws_ls2js.html)

#### Symbolic parameters

The following symbolic parameters are defined in BBGLS2JS:

**WLPDIR=path** A required parameter that specifies the name of the WebSphere Application Server Liberty directory in the UNIX System Services file system.

**TMPDIR=tmpdir** Specifies the location of a directory in IBM z/OS Unix System Services that BBGLS2JS uses as a temporary workspace. The user ID used to run the job must have read and write permission to this directory. It is an optional parameter and if it is not specified, the default value is `/tmp`.

You specify an absolute path for a Java API to use a new temporary workspace when you code the `java.io.tmpdir` custom property. For scripts, you specify the environment variable **TMPDIR** to point to this new temporary directory.

**TMPFILE=tmpprefix** Specifies a prefix that BBGLS2JS uses to construct the names of the temporary workspace files. It is an optional parameter and if it is not specified, the default value is LS2JS.

## Input Parameters

The input parameters that are documented for DFHLS2JS are also applicable to BBGLS2JS. The value that is specified for the **PGMNAME** parameter is used in the generated JSON schema.

The following example shows how to create the JCL to run the BBGLS2JS tool:

```
//LS2JS JOB 'accounting information',name,MSGCLASS=A
//JCLLIB JCLLIB ORDER=EXAMPLE.DSNAME
//JAVAPROG EXEC BBGLS2JS,
// WLPDIR='/opt/IBM/wlp'
//INPUT.SYSUT1 DD *
PDSLIB=TEST.DSNAME
REQMEM=CDATA2
RESPMEM=CDATA2
MAPPING-LEVEL=3.0
MINIMUM-RUNTIME-LEVEL=3.0
CHAR-VARYING=COLLAPSE
STRUCTURE=(requestData,requestData)
JSON-SCHEMA-REQUEST=/u/user1/json/getcustc_request.json
JSON-SCHEMA-RESPONSE=/u/user1/json/getcustc_response.json
LANG=C
LOGFILE=/u/user1/wsbinding/getcustc.log
URI=http://myserver.example.org:8080/exampleApp/example
PGMINT=COMMAREA
PGMNAME=GETCUSTC
WSBIND=/u/user1/getcustc.wsbinding
/*
```

## BBGJS2LS: JSON schema to high-level language conversion for z/OS Connect data transformation

The BBGJS2LS JCL procedure generates a high-level language data structure and binding file from a JSON schema. The files that are generated are used by the z/OS Connect data transformation process. It is based on DFHJS2LS from the CICS Transaction Server Mobile Extensions feature pack.

See the documentation for usage information and examples on using the BBGJS2LS tool. Where the documentation refers to DFHJS2LS, use BBGJS2LS. [http://www-01.ibm.com/support/knowledgecenter/SSGMCP\\_5.1.0/com.ibm.cics.ts.mobileextensions.doc/reference/dfhws\\_js2ls.html](http://www-01.ibm.com/support/knowledgecenter/SSGMCP_5.1.0/com.ibm.cics.ts.mobileextensions.doc/reference/dfhws_js2ls.html)

## Symbolic parameters

The following symbolic parameters are defined in BBGJS2LS:

**WLPDIR=path** A required parameter that specifies the name of the WebSphere Application Server Liberty directory in the UNIX System Services file system.

**TMPDIR=tmpdir** Specifies the location of a directory in z/OS UNIX that BBGJS2LS uses as a temporary workspace. The user ID used to run the job must have read and write permission to this directory. It is an optional parameter and if it is not specified, the default value is /tmp.

**TMPFILE=tmpprefix** Specifies a prefix that BBGJS2LS uses to construct the names of the temporary workspace files. It is an optional parameter and if it is not specified, the default value is JS2JS.

## Input Parameters

The input parameters that are documented for DFHJS2LS are also applicable to BBGJS2LS. The value that is specified for the **PGMNAME** parameter is used in the name of the generated high-level language structure.

The following example shows how to create the JCL to run the BBGJS2LS tool:

```
//JS2LS JOB 'accounting information',name,MSGCLASS=A
// SET QT=''
//JCLLIB JCLLIB ORDER= EXAMPLE.DSNAME
//JAVAPROG EXEC BBGJS2LS,
// WLPDIR='/opt/IBM/wlp'
//INPUT.SYSUT1 DD *
PDSLIB=TEST.DSNAME
REQMEM=CPYBK1
RESPMEM=CPYBK2
JSON-SCHEMA-REQUEST=example.json
JSON-SCHEMA-RESPONSE=example.json
LANG=COBOL
LOGFILE=/u/exampleapp/wsbinding/example.log
MAPPING-LEVEL=3.0
CHAR-VARYING=NULL
INLINE-MAXOCCURS-LIMIT=2
PGMNAME=DFH0XCMN
URI=exampleApp/example
PGMINT=COMMAREA
SYNCONRETURN=YES
WSBIND=/u/exampleapp/wsbinding/example.wsbinding
/*
```

## Auditing and tracking with z/OS Connect



Audit and track requests with z/OS<sup>®</sup> Connect, which includes an interceptor that records data to the z/OS SMF data store.

### About this task

You can enable the interceptor in z/OS Connect on a single or group of z/OS Connect services. The z/OS Connect audit interceptor records request activity to the SMF data store on z/OS operating systems. SMF type 120, subtype 11 records are generated.

The SMF data in the 120-11 record contains the standard header for SMF records. Then, there are two triplets. The first triplet points to the server identification section of which there is one instance. The second triplet points to the user data section of which there can be multiple instances.

**The server data section consists of the following parameters: (values in decimal)**

- Offset Length Data
- 0 4 Version (1)
- 4 8 System name
- 12 8 Sysplex name
- 20 8 Job id(jsabjbid)
- 28 8 Job name (jsabjbnm)
- 36 8 SToken (assbstkn)

**The user data consists of the following parameters (values in decimal):**

- Offset Length Data
- 0 4 Version (1)

- 4 4 Type
- 8 4 Length of data (user data sections are 2 K, this field indicates how much of that is used)
- 12 ? Data

**The user data consists of the following parameters (values in decimal):**

For z/OS Connect the user data type is 102 (decimal). The data contains the following parameters:

- Offset length Data
- 0 4 Version (3)
- 4 8 Arrival time (STCK format)
- 12 8 Completion time (STCK format)
- 20 64 Target URI (EBCDIC, right-padded with blanks)
- 84 4 Input payload length in bytes
- 88 64 Service name (EBCDIC, right-padded with blanks)
- 152 8 Method (EBCDIC)
- 160 4 Respond length in bytes
- 164 64 User name (EBCDIC, right-padded with blanks)
- 228 23 Request id (bytes, right-padded with zeros)
- 251 1 Boundary padding (zero)
- 252 64 Service grouping name (EBCDIC, right-padded with blanks)
- 316 8 Mapped user name (EBCDIC, right-padded with blanks) Only valid on version 3 or later.

**Procedure**

1. Enable the z/OS Connect-provided audit interceptor for a service or set of services. The z/OS Connect-supplied audit interceptor implements the `com.ibm.wsspi.zos.connect.Interceptor` SPI to store auditing/tracking information in the z/OS System Management Facility (SMF) data sets. The following is an example that shows how to enable the audit interceptor for a single service:

```
<!-- Audit interceptor configuration -->
<auditInterceptor id="auditInterceptor" sequence="1"/>

<!-- Interceptor list configuration -->
<zosConnectInterceptors id="interceptorList1" interceptorRef="auditInterceptor"/>

<!-- z/OS Connect service definitions -->
<zosConnectService id="zcs1" serviceName="recordOpsCreate" serviceRef="wolaOpsCreateService"
interceptorsRef="interceptorList1"/>
```

2. Retrieve live statistic data. Feature start time, total number of service requests and the distribution of requests are available by using this operational capability. Valid authenticated clients are able to use a HTTP GET for one of the following URIs to retrieve statistics about the z/OS Connect server:

- Get statistics for a single service:  
`https://<hostname:port>/zosConnect/services/HelloWorld?action=getStatistics`
- Get statistics for all services in the server:  
`https://<hostname:port>/zosConnect/operations/getStatistics`
- Get statistics for all services under a single service provider by specifying the `provider=<service provider name>` query parameter. For example to retrieve statistics for all services associated with the provider name of **WOLA-1.0** use the following URL:  
`https://<hostname:port>/zosConnect/operations/getStatistics?provider=WOLA-1.0`
- The response data is returned in JSON object format.

---

## Developing EJB applications on Liberty

8.5.5.6

An Enterprise JavaBeans (EJB) application is a set of beans that are packaged a combination of a Java archive file (jar), web application archive file (war), or Java EE enterprise application archive file (EAR).

### About this task

The WebSphere® Application Server Liberty provides full support for the Enterprise JavaBeans specification. The EJB Specification also defines a lite subset, which is also a configurable feature provided in Liberty in addition to several other optional features that enable server configurations that only support subsets of the full EJB specification. These subsets enable the use of server configurations that use fewer resources when all capabilities of the EJB specification are not used by the installed applications.

For information about developing EJB applications by using WebSphere Developer Tools, see [Developing EJB 3.x applications](#).

### Enterprise JavaBeans core features

#### ejbLite

This feature enables the lite subset of the EJB technology as defined in the EJB specification. This subset includes support for local session beans that are written to the EJB 3.x APIs. Beginning with the `ejbLite-3.2` feature, the subset also includes support for non-persistent EJB timers and asynchronous local interface methods.

Other than enabling the `ejbLite-3.2` feature in the `server.xml` file, no additional configuration is required for this feature.

#### mdb

This feature enables the message-driven bean subset of the EJB technology, which is similar to the support that the `ejbLite` feature enables for session beans. The feature does not enable session beans, so if both session and message-driven beans are needed, then both features need to be enabled in the `server.xml` file.

The following features provide the minimum set of capabilities for the EJB APIs:

**Note:** EJB 2.x API entity beans are not supported by Liberty. For persistence, the Java Persistence API (JPA) must be used instead.

### Enterprise JavaBeans extension features

The following features provide extensions to the core EJB features, which, when they are combined, provide support for the full set of EJB APIs:

#### ejbHome

Enables support of the EJB 2.x APIs, specifically, support for the `javax.ejb.EJBLocalHome` interface. The `javax.ejb.EJBHome` interface is also supported when combined with the `ejbRemote` feature. Since this feature is not useful without the `ejbLite` feature, enabling this feature automatically enables the corresponding `ejbLite` feature.

Other than enabling the feature in the `server.xml` file, no additional configuration is available for this feature.

#### ejbPersistentTimer

Enables support for persistent EJB timers. Enabling this feature automatically enables the corresponding `ejbLite` feature.

In addition to enabling this feature in the `server.xml` file, a data source must also be configured to provide the persistent store for the timers. By default, the `DefaultDataSource` is used, so that configuration is all that is required.

### **ejbRemote**

Enables support for remote EJB interfaces. Enabling this feature automatically enables the corresponding `ejbLite` feature.

Other than enabling the feature in the `server.xml` file, no additional configuration is required for this feature.

### **Enterprise JavaBeans convenience feature**

The following feature provides a convenient way to enable the full set of EJB APIs:

#### **ejb**

Enables all of the core and extension features for the specification level of the configured feature. For example, `ejb-3.1` enables `ejbLite-3.1` and `mdb-3.1`. This feature provides no additional support beyond what is provided by enabling all of the core and extension EJB features.

Other than enabling the feature in the `server.xml` file, no additional configuration is required for this feature.

### **Procedure**

Enable the feature in the `server.xml` file. For example:

```
<featureManager>
  <feature>ejbLite-3.2</feature>
</featureManager>
```

## **Developing Enterprise bean (EJB) persistent timer applications**

8.5.5.6

EJB persistent timers are created either automatically by the container or programmatically by an application. Both types of persistent timers are stored in tables in the database that is configured for the EJB timer service in the `server.xml` file.

### **About this task**

After the persistent timer is created, it exists in the database until one of the following occurs:

- The timer is not scheduled for further expirations; for example, after a single-action timer expires and runs successfully.
- The timer is canceled by the application.
- The timer is canceled by using the EJB timer service MBean (`EJBPersistentTimerServiceMBean`)
- The timer is manually removed from the database. For example, if the timer service database is cleared or removed.

Also, note that EJB persistent timers are associated with an EJB based on the application name, module name, and bean name. If an application is updated, and any of these names change, then the timer continues to exist in the database, but appears to no longer exist as it no longer expires and runs.

The Enterprise JavaBeans specification declares that automatic timers are created by the container when an application is deployed. For Liberty, this occurs the first time that an application starts within a server process. During the first application start, the automatically created persistent timers are stored in the persistent timer database along with an indication that the application has been deployed. The container does not create the automatic persistent timers again until both the timers and the indication that the

application has been deployed is removed from the EJB persistent timer database.

## Procedure

Enable the EJB persistent timer feature in the `server.xml` file; for example:

```
<featureManager>
  <feature>ejbPersistentTimer-3.2</feature>
</featureManager>
```

## Managing enterprise beans (EJB) persistent timers

8.5.5.6

Applications or modules can create EJB persistent timers either automatically or programmatically that are stored in a database. An MXBean is provided for viewing the persistent timers that exist in the database and removing some or all persistent timers that are associated with an application.

### About this task

The best way to manage EJB persistent timers is through the application that created the timers. The application that created the timer is able to provide the context of why the timer was created and exactly what action the timer performs when the timer reaches the expiration. However, for application development and diagnostic purposes the EJB timer service does provide an MXBean capable of performing basic timer management functions, `com.ibm.websphere.ejbcontainer.mbean.EJBPersistentTimerServiceMXBean`.

The MXBean provides operations to find the EJB persistent timers that are associated with an application, module, or specific bean. The viewable information includes the name of the bean that the timer is associated with and the schedule when the timer expires. Application-specific data that is associated with the timer might not be viewable. Operations are also provided to cancel a specific timer or all timers that are associated with an application, module, or bean.

The EJB APIs do not provide a mechanism for providing a unique identity when creating timers, however when the timer is stored in the database a unique identity is associated with the timer and used as the primary key into the database. There is no way to programmatically obtain the timer identity, but the identity is part of the viewable information provided by the MXBean 'get' operations. The identity appears in logs when an error is encountered involving the timer. And, the identity is the value that is used to cancel a specific timer through the '`cancelTimer`' MXBean operation.

Note: All MXBean operations perform the same for both automatic and programmatic persistent timers.

## Procedure

1. Configure the application server to include an EJB feature that supports persistent timers and the rest connector in the `server.xml` file.

```
<featureManager>
  <feature>servlet-3.1</feature>
  <feature>ejbPersistentTimer-3.2</feature>
  <feature>jdbc-4.1</feature>
  <feature>restConnector-1.0</feature>
</featureManager>
```

2. Start the JConsole from the JVM bin directory and connect to the Liberty server process.
3. Navigate to the EJB timer service MXBean.
4. Enter the application name in the **String** field of the first '`getTimers`' operation and submit to receive information about the persistent timers for the application.

## Managing automatically created EJB persistent timers

8.5.5.6

Applications or modules use the `javax.ejb.Schedule` annotation or the `schedule` element in the XML deployment descriptor to instruct the application server to automatically create EJB timers. An MBean is provided for managing the creation of the automatically created EJB persistent timers.

## About this task

The Liberty server creates the EJB automatic persistent timers for an application the first time the application is started within the server process. The timers, and an indication that they have been created, are stored in the database associated with the `PersistentExecutor`, configured for the EJB timer service. Once created, the automatically created persistent timers for an application will not be created again until an action is taken to specifically clear the indication that they have been created from the database. Even if all of the automatically created timers for an application are removed, the Liberty server will not create any of them again until the indication that they have been created is also removed.

Clearing the indication that the automatically created timers have been created may be done by either manually clearing the timer database or using the EJB timer service MBean. The EJB timer service MBean can be used either programmatically or through a tool such as JConsole. The interface for the EJB timer service MBean is: `com.ibm.websphere.ejbcontainer.mbean.EJBPersistentTimerServiceMXBean`.

## Procedure

1. Configure the application server to include an EJB feature that supports persistent timers and the rest connector in the `server.xml` file.

```
<featureManager>
  <feature>servlet-3.1</feature>
  <feature>ejbPersistentTimer-3.2</feature>
  <feature>jdbc-4.1</feature>
  <feature>restConnector-1.0</feature>
</featureManager>
```

2. Configure the application server to include a datasource for the EJB timer service in the `server.xml` file.

```
<dataSource id="DefaultDataSource" jdbcDriverRef="DerbyEmbedded">
  <properties.derby.embeddedcreateDatabase="create" databaseName="\${server.config.dir}/data/EJBTimerDB"/>
</dataSource>
<jdbcDriver id="DerbyEmbedded" libraryRef="DerbyLib"/>
<library id="DerbyLib">
  <filename="\${server.config.dir}/derby/derby.jar"/>
</library>
```

3. Obtain the MBean server connection.

4. Obtain the EJB persistent timer service MBean.

```
import javax.management.MBeanServerConnection;
import javax.management.ObjectName;
import com.ibm.websphere.ejbcontainer.mbean.EJBPersistentTimerServiceMXBean;
...
MBeanServerConnection mbsc = <step #3>;
ObjectName on = new
ObjectName("WebSphere:feature=ejbPersistentTimer,type=EJBPersistentTimerService,name=EJBPersistentTimerService");
EJBPersistentTimerServiceMXBean timerServiceMBean =
    JMX.newMXBeanProxy(mbsc, on, EJBPersistentTimerServiceMXBean.class);
```

5. Remove the automatically created persistent timers for the application.

```
timerServiceMBean.removeAutomaticTimers("<application name>");
```

The `removeAutomaticTimers()` method on the MBean removes both the automatically created timers and the indication that they were created. The next time that the server starts the application, the automatically created persistent timers are created.

## Configuring the enterprise JavaBeans timer service for persistent timers

8.5.5.6

For persistent EJB timers, you can configure the EJB timer service to control the data source where the timers are stored, the interval between timer retries and the number of retry attempts for failed calls to the timeout callback method.

## About this task

When the `ejbPersistentTimer` feature is enabled, a data source must be configured for persisting the timers or any attempt to use persistent timers fails. The EJB timer service uses the `DefaultDataSource` if it is configured and no other specific data source is configured for use by the EJB timer service.

Also, the EJB timer service retries failed calls to the timeout callback method for persistent timers every 5 minutes until the timeout callback method completes successfully.

Use the following options to configure persistent timers.

### EJB Persistent Timers Scheduled Executor

Specifies a reference to a persistent executor that controls the behavior of persistent timers. A default instance, `defaultEJBPersistentTimerExecutor`, is provided which uses the `DefaultDataSource` as the persistent store. The EJB persistent timers scheduled executor reference might be changed to a custom configuration, or the default instance might be overridden to change specific values. The following options are available for the persistent executor:

#### Retry limit

Specifies the maximum number of times that the failing timeout callback method might be retried. If the timeout callback method is successful upon retry, the server stops attempting to run it. If a retry fails, the server continues to attempt retries until the timeout callback method succeeds, or the retry limit is reached. After the retry limit is reached, the server does not attempt to run the timeout callback method, even if prior attempts did not succeed. The default value of -1 indicates unlimited retries. A value of 0 indicates no retries, and is not compliant with the EJB specification. A value of 1 or greater indicates the specific number of retries.

Changing the configuration of the number of times a timeout callback method is retried for non-persistent timers is useful for applications that do not require non-persistent timers to complete at each of the scheduled times. For example, if an application creates a non-persistent interval timer that is scheduled to run every 5 minutes, then configuring the number of retries to 0 results in the timer, running one time every 5 minutes, regardless of whether it succeeds or fails.

#### Retry interval

Specifies the interval between retry attempts for a failed timeout callback method. The first retry always occurs immediately, regardless of the interval that is configured for this value. All additional retries wait for the interval that is specified for this value. A value of 0 indicates that all retries are immediate. A value of 1 or greater indicates that retries must wait for that specific number of seconds. The default is 300 seconds.

Configuring a different time interval between retries for non-persistent timers is useful for applications where it is important for the timeout callback method to complete before the scheduled time. This approach is also applicable for applications where it is acceptable to delay the timer completion to a later time, such as a later retry interval, to enable the timeout callback method so the application can have a better chance to run successfully.

#### Persistent Task Store

Specifies which data source is used. A default instance, `defaultDatabaseStore`, is provided which uses the `DefaultDataSource` as the persistent store.

## Procedure

1. Configure the application server to include an EJB feature that supports persistent timers in the `server.xml` file.

```
<featureManager>
  <feature>ejbPersistentTimer-3.2</feature>
</featureManager>
```

2. Configure the EJB timer service to use a specific maximum number of retry values and retry interval values for persistent timers in the `server.xml` file. For example, use the following configuration to specify that the persistent timers retry up to 3 times, with 10 seconds between retries:

```
<persistentExecutor id="defaultEJBPersistentTimerExecutor" retryInterval="10s"
  retryLimit="3"/>
```

With this configuration, the timeout callback method for a timer can be called up to 4 times. The first call occurs at the scheduled time. If the first call fails, then the first retry occurs immediately after the failure. If the timeout callback method continues to fail, then the second and third retries occur 10 and 20 seconds later.

In the following example, a failed timeout callback method is only retried one time. The callback interval is irrelevant because the first retry is always started immediately.

```
<persistentExecutor id="defaultEJBPersistentTimerExecutor" retryLimit="1"/>
```

3. Configure the EJB timer service to use a specific data source for persistent timers in the `server.xml` file. For example, use the following configuration to specify that the persistent timers must be stored by using the `jdbc/timerDataSource`.

```
<databaseStore id="EJBTimerDatabaseStore" tablePrefix="EJBTimer_"/>
<persistentExecutor id="defaultEJBPersistentTimerExecutor"
  taskStoreRef="EJBTimerDatabaseStore"/>
```

## Configuration options for persistent enterprise JavaBeans timers: 8.5.5.6

Persistent EJB timers do not require any configuration beyond enabling the `ejbPersistentTimer` feature and setting up the default data source, which has an ID of `DefaultDataSource`, to point to a database. Optional configuration settings are available to control behaviors such as choosing a different data source, controlling when and how often the database is polled to look for persisted timer tasks, and whether and how often to retry failed or rolled back timer tasks.

EJB timer configuration is specified by an optional `timerService` configuration element. Configuration attributes for persistent EJB timers are further grouped under a `persistentExecutor` configuration. By default, the EJB timer service uses a persistent executor instance named `defaultEJBPersistentTimerExecutor`. It is possible to customize the EJB persistent timer configuration by configuring the timer service to use a different persistent executor instance. However, the best practice for customizing the EJB persistent timer configuration is to override the `defaultEJBPersistentTimerExecutor` instance so that you inherit default values from the `defaultEJBPersistentTimerExecutor` instance.

For example, to override only the retry limit,

```
<persistentExecutor id="defaultEJBPersistentTimerExecutor" retryLimit="50"/>
```

### Customizing the database store for persistent timer tasks

Persistent EJB timer tasks are persisted to a database. Configuration related to the database is grouped under the `databaseStore` configuration element. Unless configured otherwise, an instance of `databaseStore` named `defaultDatabaseStore` is used for persistent EJB timers as well as by other product features that require a database. An example of overriding the `defaultDatabaseStore` instance,

```
<databaseStore id="defaultDatabaseStore" dataSourceRef="DB2DataSource" tablePrefix="MYTIMERS"/>
```

An example of configuring the `defaultEJBPersistentTimerExecutor` instance to use a different `databaseStore` instance,

```
<persistentExecutor id="defaultEJBPersistentTimerExecutor" taskStoreRef="MyDBStore"/>
<databaseStore id="MyDBStore" dataSourceRef="DB2DataSource" tablePrefix="MYTIMERS">
  <authData user="user1" password="password1"/>
</databaseStore>
```

### Enabling and disabling persistent timer task execution

Persistent EJB timer tasks are enabled to run upon commit of the transaction from which they are scheduled. To prevent persistent timer tasks from running, you can configure the `enableTaskExecution` attribute with a value of `false`, in which case the EJB timer service still writes persistent timer tasks to the database but does not run them. If the value is switched to `true`, the EJB timer service will start running the timers that were previously scheduled as well as any new timers that are scheduled.

### Customizing polling of the persistent store for timer tasks

A single initial poll of the persistent store is performed upon startup to locate any previously scheduled timer tasks. When tasks are scheduled, information about the scheduled next run time is persisted as well as kept in memory, making it unnecessary to do further polling of the persistent store. This behavior is ideal in many cases, but might not always be desirable.

- If the timer tasks have external dependencies on other services, the initial poll might occur too soon and timer tasks might fail due to the external services they require being unavailable. If this happens, an initial poll delay can be used to defer the initial poll by a fixed amount of time.
- If a large number of EJB persistent timers are scheduled, they might consume too much memory. In this case, you can configure a poll interval to periodically poll the persistent store for only the timer tasks that you want to run within the interval up until the next poll. The poll size further limits the number of timer tasks that can be read from the database each poll interval, which might cause some tasks to run late.

Example configuration:

```
<persistentExecutor id="defaultEJBPersistentTimerExecutor" initialPollDelay="5m" pollInterval="10m" pollSize="200"/>
```

### Retries for failed and rolled back persistent timer tasks

When persistent EJB timer executions fail or are marked to roll back, they are retried one time immediately. If the immediate retry fails, they are retried at a fixed interval until successful. It is possible to limit the number of retry attempts by specifying a retry limit in the configuration. You can also control the interval between retries by specifying a retry interval in the configuration.

Example configuration:

```
<persistentExecutor id="defaultEJBPersistentTimerExecutor" retryLimit="100" retryInterval="2m"/>
```

## Using enterprise JavaBeans with remote interfaces on Liberty

8.5.5.6

You can remotely access Enterprise Java™ Bean (EJB) methods with remote interfaces when the EJB is hosted by another Java virtual machine (JVM) or another application within the same JVM. WebSphere® Application Server implements remote EJB interfaces by using RMI-IIOP technologies. You can enable remote EJB support with the `ejbRemote-3.2` feature.

### About this task

To configure a Liberty server to run an application with remote EJB support enabled, you must set the `ejbRemote-3.2` feature.

When you use remote EJB interfaces, review the following considerations:

#### Naming

## Using the java: namespace

The EJB specification requires that remote interfaces are bound to the java: namespace; for example:

```
java:global/ExampleApp/ExampleModule/ExampleBean!com.ibm.example.ExampleRemoteInterface
java:app/ExampleModule/ExampleBean!com.ibm.example.ExampleRemoteInterface
java:module/ExampleBean!com.ibm.example.ExampleRemoteInterface
```

EJB components are not bound to the default Java Naming and Directory Interface (JNDI) namespace as in WebSphere Application Server traditional, so @EJB lookups and bindings in ibm-\*.bnd.xml files must not use this namespace. These lookups must use the java: names for EJB components that are hosted within the same server, and corbaname: URLs for EJB components that are hosted in another server.

## Using corbaname: URLs

Interfaces are also bound to the ORB CosNaming name service in similar contexts to those interfaces used in the java:global namespace. These interfaces can be accessed through JNDI by using corbaname: URLs; for example:

```
corbaname::test.ibm.com:2809#ejb/global/ExampleApp/ExampleModule/ExampleHomeBean!com.ibm.example.ExampleEJBHome
corbaname:rir:#ejb/global/ExampleApp/ExampleModule/ExampleHomeBean!com.ibm.example.ExampleEJBHome
```

On the server, the rir: form of the URL uses the local name service. On the client, it uses the default or configured remote name service.

## Escaping corbaname: URLs

According to the Object Management Group (OMG) Naming Service specification, some characters in corbaname: URLs must be escaped. Liberty tries to determine whether a corbaname: URL that is derived from the java:global namespace needs to be escaped, and then escapes it automatically. It is not possible to do the escape in all cases. For example, if a name contains a single dot (.), and has no invalid characters, it cannot be escaped automatically. To force a name to be interpreted in a particular way, it is necessary to escape the URL manually as described in the OMG Naming Service specification.

Consider the following java:global name for an enterprise bean:

```
java:global/TestApp/TestModule/TestBean!test.TestRemoteInterface
```

The simple form of the corbaname: URL cannot be escaped automatically because it represents a different, but valid location. Therefore, the following URL does not work as expected:

```
corbaname:rir:#ejb/global/TestApp/TestModule/TestBean!test.TestRemoteInterface
```

Instead, this URL must be manually escaped as follows:

```
corbaname:rir:#ejb/global/TestApp/TestModule/TestBean!test%5c.TestRemoteInterface
```

The syntax for escaping corbaname: URLs is described fully in OMG Naming Service specification.

## Using JNDI names programmatically

All of the URLs and JNDI names in these examples can be looked up programmatically from an InitialContext. When you look up a java: name, the resulting object can be cast directly to the expected type; for example:

```
Object found = new InitialContext().lookup("java:global/ExampleApp/ExampleModule/ExampleBean!com.ibm.example.ExampleRemoteInterface");
ExampleRemoteInterface bean = (ExampleRemoteInterface) found;
```

However, when you retrieve objects by using corbaname: URLs, the RMI style of casting, called narrowing, must be used; for example:

```
Object found = new InitialContext().lookup("corbaname:rir:#ejb/global/ExampleApp/ExampleModule/ExampleBean!com.ibm.example.ExampleRemoteInterface");
ExampleRemoteInterface bean = (ExampleRemoteInterface) PortableRemoteObject.narrow(found, ExampleRemoteInterface.class);
```

## Interoperability

Any product that supports the IIOP protocol can call enterprise beans that use the EJB 2.x remote

programming model with EJBHome and EJBObject when it is packaged in an EJB JAR module with a version 2.0 deployment descriptor. The `WLP_INSTALL_DIR/clients/ejbRemotePortable.jar` file must be included on the class path of the remote client. This file contains system value classes that are required for communication with a Liberty server. This file is not required when you remotely access EJB components from Liberty or WebSphere Application Server traditional. EJB components that use the EJB 3 remote programming model on Liberty can be remotely accessed by WebSphere Application Server processes. Liberty does not provide a thin client to start EJB components from a stand-alone Java process. Liberty does not provide workload management or failover capabilities for remote EJB components, including when you start EJB components that are hosted from WebSphere Application Server traditional.

### Stub classes

A client must include stub classes when you start a remote EJB that is hosted on an WebSphere Application Server. In some cases, if the client is WebSphere Application Server, the product automatically generates the correct stub classes:

- If a client application starts a remote EJB that is contained within the same application, then Liberty automatically generates stub classes.
- If the target EJB is running in a separate application and is using the EJB 2.x remote programming model with EJBHome and EJBObject, then the client must include stub classes on its classpath. If the EJB is hosted on WebSphere Application Server traditional, you can copy the EJB client JAR from the application from the EAR after it is processed by the `ejbdeploy` command. If the EJB is hosted on WebSphere Application Liberty, you must use the `rmic` program that is included with your Java SDK to generate the stub classes for the target EJB, and then you must include the stub classes with the client.
- If the target EJB is running in a separate application and is using the EJB 3 remote programming model, then the client WebSphere Application Server Liberty or WebSphere Application Server traditional process automatically generates stub classes. EJB components that use the EJB 3 remote programming model on Liberty can be remotely accessed by WebSphere Application Server or WebSphere Application Client processes only.

### Transaction propagation

Liberty does not support outbound or inbound transaction propagation. Additionally, the EJB specification requires that, even if a product supports outbound transaction propagation, it must still send a null transaction context. This context must be rejected by EJB components that use the Required (default), Mandatory, or Supports transaction attributes. A client with an active global transaction cannot start an EJB with default transaction attributes if either the client or server is in Liberty. The client can start the EJB if the EJB is changed to use the RequiresNew or NotSupported transaction attributes. However, the transactional work that is done by the EJB is not committed as part of the transactions of the client.

### Asynchronous methods

An EJB remote interface can have an asynchronous method with a return value of type Future. The server will return a Future object to the client, which is used to retrieve the value. Remote asynchronous methods are not recommended because accumulation of unclaimed results can exhaust memory. To mitigate this problem, the server results expire if the client does not retrieve the result within 24 hours or if the maximum number of unclaimed results exceeds 1000. These values can be adjusted in the `server.xml` file; for example:

```
<ejbContainer>
  <async maxUnclaimedRemoteResults="10"unclaimedRemoteResultTimeout="10m"/>
</ejbContainer>
```

### Procedure

1. To enable this feature, update the `server.xml` file to add the `ejbRemote-3.2` feature; for example:

```
<featureManager>
  <feature>ejbRemote-3.2</feature>
</featureManager>
```

2. Configure your application binding files, `ibm-*-bnd.xml` files, for remote EJB references that have been defined either in the deployment descriptor `<ejb-ref>` or with source code annotations, `@EJB`. A binding is not required for EJB references that provide a lookup name, either on the annotation or in the deployment descriptor. In the binding file, the EJB reference can be bound using one of the `java:` names for an EJB or with one of the `corbaname:names`; for example:

For an EJB reference:

```
@EJB(name="TestBean")
    TestRemoteInterface testBean;
```

The binding is defined:

```
<ejb-ref name="TestBean" binding-name="corbaname:rir:#ejb/global/TestApp/TestModule/TestBean!test%5c.TestRemoteInter
```

3. Configure your application client to include stub classes.
4. (Optional) Configure interoperability for applications that support the IIOP protocol to use EJB remote interfaces by adding the `WLP_INSTALL_DIR/clients/ejbRemotePortable.jar` file on the class path of the remote client.

## Using enterprise JavaBeans applications that call local EJB components in another application

8.5.5.6

The Enterprise JavaBeans (EJB) specification requires that local client views are supported for EJB components that are packaged within the same application. This includes local homes, local business interfaces, and the no-interface view. Local client views are also supported for EJB components that are not packaged within the same application, but additional configuration is required.

### About this task

The product supports access to local client views to EJB components packaged within a separate application with some restrictions:

- The local interface and all parameter, return, and exception types that are used by the local interface must be visible to the class loader of both the calling application and the target EJB application. You can ensure that they are visible by either using a shared library that is associated with a server class loader or by using a common library reference with both applications.
- When the target EJB application is stopped, any cached references to the EJB must be refreshed by restarting the calling application. The simplest solution is to restart the calling application whenever you restart a target EJB application on which it relies.

### Procedure

Add the configuration to the `server.xml` file; for example:

```
<library id="ejbInterfaceLib">
  <file name="${server.config.dir}/lib/ejbInterfaceLib.jar"/>
</library>
<webApplication id="ejbClient" location="ejbClient.war">
  <classloader commonLibraryRef="ejbInterfaceLib"/>
</webApplication>
<ejbApplication id="ejbApp" location="ejbApp.ear">
  <classloader commonLibraryRef="ejbInterfaceLib"/>
</ejbApplication>
```

---

## Developing SIP applications on Liberty

8.5.5.7

A Session Initiation Protocol (SIP) application is a set of SIP servlets that are packaged in a SIP application archive file (SAR).

## About this task

A SIP servlet is an application component that is managed by the SIP container that performs SIP signaling. The programming and deployment models are analogous to web servlets and are therefore mapped to the Liberty administrative model. You can include web servlets in a SAR file (along with the required web.xml deployment descriptor) to create what is known as a converged application. See JSR 116 and JSR 289 for details on SIP applications, servlets, converged applications, and status codes.

You can use developer tools, such as the IBM WebSphere Application Server Developer Tools for Eclipse, to develop SIP servlets using graphical deployment descriptor editors and basic wizards. The developer tools also include other features that integrate with Liberty deployments, such as tools for server automation and application packaging. For more information, see WebSphere Developer Tools > Developing > Developing SIP applications.

## Developing SIP applications that support PRACK on the Liberty

8.5.5.7

A SIP response to an INVITE request can be final or provisional. Final responses are always sent reliably, but provisional responses typically are not. For cases where you need to send a provisional response reliably, you can use the PRACK (Provisional response acknowledgment) method.

### Before you begin

To develop applications that support PRACK, the following criteria must be met:

- To indicate that the client supports PRACK, the client that sends the INVITE request must put a 100rel tag in the Supported or the Require header.
- The SIP servlet must respond by invoking the sendReliably() method instead of the send() method.

### About this task

PRACK is described in the following standards:

- RFC 3262 (“Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”), which extends RFC 3261 (“SIP: Session Initiation Protocol”), adding PRACK and the option tag 100rel.
- Section 5.7.1 (“Reliable Provisional Responses”) of JSR 289 (“SIP Servlet Specification Version 1.1”).

### Procedure

- If you are developing an application that acts as a proxy, make your application generate and send a reliable provisional response for any INVITE request that has no tag in the To field.
- If you are developing an application that acts as a user agent client (UAC), perform the following actions:
  - Make your application add the 100rel tag to outgoing INVITE requests. The option tag must appear in either the Supported header or the Require header.
  - To create a PRACK request and send the request to the user agent server (UAS), invoke the createPrack() method on the incoming response within your application's doProvisionalResponse(...) method. The container handles the RAck header as defined in JSR 289 Section 5.7.1.
  - The application that acts as an UAC receives a final 2xx-6xx response on the PRACK, which the UAC can handle with a doResponse() method.
- If you are developing an application that acts as a user agent server (UAS), perform the following actions:
  -

**Note:** If an incoming INVITE request requires the 100rel tag, trying to send a 101-199 response unreliably by using the send() method causes an exception.

- In the application, declare a SipErrorListener object to receive noPrackReceived() events when a reliable provisional response is not acknowledged within 64\*T1 seconds, where T1 is a SIP timer. Within the noPrackReceived() event processing, the application generates and sends a 5xx error response for the associated INVITE request per JSR 116 Section 6.7.1.
- The application can have at most one outstanding, unacknowledged reliable provisional response. Trying to send another one before the first is acknowledged results in an exception.
- Make sure that the application enforces the RFC 3262 offer/answer semantics for PRACK requests containing session descriptions. Specifically, a servlet must not send a 2xx final response if any unacknowledged provisional responses contained a session description.

## Developing back-to-back (B2B) applications

8.5.5.7

You can use the javax.servlet.sip.B2buaHelper interface to develop a Back-to-Back User Agent (B2BUA) application.

### Before you begin

Read the JSR289 specification, section 12, which provides detailed information about the B2BUA operations. The SIP Servlet 1.1 specification defines a helper class, javax.servlet.sip.B2buaHelper, for creating B2BUA applications. For more information, see the documentation on the B2buaHelper methods.

### About this task

The B2BUA is a Session Initiation Protocol (SIP) application that sits in the middle of a SIP call, and forwards requests and responses between two or more SIP dialogs. A typical B2BUA application manages SIP sessions between two user agents. However, the B2BUA application can also handle more complex scenarios where it needs to manage responses from different branches of downstream forking. Downstream forking occurs when the request is split into different branches and the message is forwarded from the user agent client to the user agent server. The B2buaHelper class contains all the necessary methods for creating such B2BUA applications. The behavior of the B2buaHelper class and the rules that are used to create new requests are defined in the JSR289 specification, section 12.2. You can use the B2buaHelper class functions for linking two legs, the incoming call leg and the outgoing call leg, of the SIP back-to-back user agent call.

### Procedure

1. Retrieve the B2buaHelper instance by calling the SipServletRequest.getB2buaHelper() method.
2. After you retrieve this instance, you can create a new SIP request by calling B2buaHelper.createRequest().

```
private void doInvite(SipServletRequest req) {  
    B2buaHelper b2buaHelper = req.getB2buaHelper();  
    SipServletRequest newRequest = b2buaHelper.createRequest(req, true, headerMap);  
}
```

The newRequest that is created is identical to the SipServletRequest req that is provided as an original request in the first parameter of this method. The **Boolean** parameter indicates whether the original request req and the newRequest are linked. The headerMap provides a map of non-system headers to override in the newRequest.

3. Ensure that the two legs are linked. If you called the createRequest method with false attribute, you can link the SIP sessions explicitly by calling:  
B2buaHelper.linkSipSessions(session1, session2)
4. After the SIP sessions and SIP requests are linked, you can retrieve the linked session by calling:

```
SipSession linkedSession = B2buaHelper.getLinkedSession(req.getSession());
```

**Note:** In B2BUA forking scenario, the application creates more than one SIP request, so not all SIP sessions are linked. You must link them explicitly.

5. After you receive a response from the User Agent Server (UAS), create a response to its leg. Check to determine whether a linked session on the response exists and if it does, use the linked request to create a response to the User Agent Client (UAC).

```
SipServletRequest linked = b2bHelper.getLinkedSipServletRequest(resp.getRequest());  
linked.createResponse(resp.getStatus(), resp.getReasonPhrase()).send();
```

If there is no linked session that is associated with the response, the application needs to call `B2buaHelper.createResponseToOriginalRequest` and create a new derived session, which is a copy of the `SipSession` that is associated with the original request.

**Note:** The JSR289 specification, section 12.5 provides a way to create more than one successful response to the original request. If there is more than one `SipSession` that is associated with the original INVITE message and there is a need to send more than one successful response to the INVITE message, then use the `B2buaHelper.createResponseToOriginalRequest` method.

6. If you use the `createResponseToOriginalRequest` method, ensure that the two legs are linked. Your application is responsible for linking the new derived session to its pair session so it can retrieve the linked session for sending subsequent responses on it.

## Developing applications that use the Asynchronous Invocation API on the Liberty profile

8.5.5.7

You can use the Asynchronous Invocation API to transfer events that require processing in the context of a Session Initiation Protocol (SIP) application session to any server in a cluster based on the related application session ID. The Asynchronous Invocation API transfers the event task to the correct server.

### Before you begin

Read the API documentation for information on the following asynchronous work classes:

- `com.ibm.websphere.sip.AsynchronousWork`
- `com.ibm.websphere.sip.AsynchronousWorkListener`

### About this task

When running code outside of a SIP thread, application developers can use the Asynchronous Invocation API to create an object. They can then configure the server to run that object either on a different thread in the same container, or on a different server, if that is where the session exists.

The following example shows the class structure for the `AsynchronousWork` class, which is the abstract base class that is extended when you use the API.

```
public abstract class AsynchronousWork implements Serializable  
{  
    private String sessionId;  
    public AsynchronousWork(String sessionId)  
    {  
        this.sessionId = sessionId;  
        ....  
    }  
    public void dispatch (AsynchronousWorkListener listener)  
    {
```

```

.....
}
public abstract Serializable doAsyncTask();
}

```

## Procedure

1. Extend the abstract class `AsynchronousWork` with the SIP-related code. The extended implementation of the `doAsyncTask()` method is invoked on the target server that contains the `SipApplicationSession`, and whose ID was set in the constructor that implements the `AsynchronousWork` class. The implementation class must pass the session ID to the base class by calling `super` in the constructor.

```

public class MyClass extends AsynchronousWork
{
String _sessionId;

public MyClass(String sessionId) {
super(sessionId);
_sessionId = sessionId;
}

// This code is invoked on the target machine or thread
public Serializable doAsyncTask() {
// Application code goes here; for instance:
appSession = sessionUtils.getApplicationSession(_sessionId);
appSession.createRequest().....

Serializable myResponse = new MyResponse();
myResponse.setStatus(200);
return (myResponse);
}
}

```

2. To receive information about the task completion, implement the `AsynchronousWorkListener` class, as in the following example. The code in these methods is invoked on the source server.

```

public class MyListener implements AsynchronousWorkListener
{
public void workCompleted(Serializable myResponse)
{
.....
}
public void workFailed(int reasonCode, String reason)
{
}
}

```

3. Invoke the asynchronous call; for example, when you receive the proprietary message, use this sample code as an example.

```

public void onMyMessage()
{
// Obtain the session ID from the message or
// somewhere else
String sessionId = obtainIdFromMessage();

// Create the runnable
MyClass myClass = new MyClass(sessionId);

// Create the listener
MyListener myListener = new MyListener();

// Dispatch it
myClass.dispatch(myListener);
}

```

## Results

The SIP container ensures that the task is invoked in the correct server and on the correct thread, so that the application can avoid synchronization on the session level.

### Asynchronous Invocation API on Liberty

8.5.5.7

Use the Asynchronous Invocation API to transfer events that require processing in a Session Initiation Protocol (SIP) application session to any server in a cluster based on an application session ID.

The Asynchronous Invocation API, also referred to as the asynchronous work dispatcher, can transfer events that require processing in the context of a SIP application session to any server in a cluster, using the related application session ID. These transfers are usually triggered by events that cause a state change to SIP sessions on another server. The asynchronous work dispatcher transfers the event task to the correct server to be run.

On Liberty, all related SIP messages are delivered to the same server in the cluster, and sessions are always in the same SIP container. To prevent synchronicity issues and locking, tasks in the same application session cannot be processed simultaneously (that is, on different threads or processes), which limits handling of certain types of events.

For more in-depth information about SIP sessions and SIP application sessions, see Section 6 of Java Specification Request (JSR) 289.

The following two scenarios are resolved by implementing the Asynchronous Invocation API.

1. Two requests that are related to the same SIP application session are simultaneously run on two different threads.

For example, a Java Platform, Enterprise Edition. application that works with a message-driven bean (MDB) can retrieve an event to send a SIP message on a certain SIP application session. At the same time, the SIP container receives an incoming SIP message on another session that is connected to the same application session and handles that on a different thread. It is necessary to synchronize the session access to avoid race conditions and to ensure that all session attributes are synchronized. To employ the locking mechanism in this case would not be effective, because the SIP application session might contain multiple SIP sessions.

2. A server that does not own a certain SIP application session receives a request, through non-SIP protocol, to send a message in the context of that session.

For example, a web service that initiates SIP dialogs can be in a server different from the server that owns the SIP application session it must use.

The Asynchronous Invocation API ensures that the specific application code is run on the correct server and correct thread according to the SIP application session ID.

The Asynchronous Invocation API provides the following benefits:

1. No more than two servers are involved in the asynchronous invocation process: one is the server that retrieves the work task, and the other is the target server that handles the SIP application session for that task and to which the task is transferred.
2. The asynchronous invocation allows working in a thread-safe manner. This approach ensures that only one thread processes the messages that are related to the SIP application session, so you do not need to synchronize access to the session.
3. The asynchronous invocation provides a scalable solution so performance is not impacted when more servers are added to the cluster.
4. Cross-server invocation is used only when required, which results in better performance.

## Performing DNS lookups in Session Initiation Protocol (SIP) applications on the Liberty profile

8.5.5.7

Use the Domain Resolver API in your application to perform Domain Name System (DNS) lookups of SIP URIs using the RFC 3263 protocol. You can perform synchronous lookups to avoid having to preserve state, which is required for an asynchronous callback. Alternatively, you can perform asynchronous lookups if you need a better performing interface.

### Before you begin

In your `server.xml` file, install and configure the `sipServlet-1.1` feature with a `domainResolver` element. For more information, see “Administering Session Initiation Protocol (SIP) on Liberty” on page 1728.

### Procedure

1. Access the Domain Resolver API in your application.

- Get an attribute from the ServletContext method using `com.ibm.websphere.sip.resolver` as a key.  
`getServletContext().getAttribute("com.ibm.websphere.sip.resolver ")`

- Use resource injection.

```
@resource
DomainResolver resolver
```

2. Perform the URI lookup.

- To use the API synchronously, call the `locate(SIPURI)` method, which returns the result of the URI resolve request response.

```
DomainResolver
locate(SIPURI)
```

- To use the API asynchronously, call the `locate(SIPURI, Listener)` method, which signals the listener after it finishes. When the result is cached, the listener is triggered on the same caller thread.

```
DomainResolver
locate(SIPURI, Listener)
```

## Receiving unmatched messages in Session Initiation Protocol (SIP) on Liberty

8.5.5.7

Use the `UnmatchedMessageListener` API to receive incoming Session Initiation Protocol (SIP) request or response messages that the SIP container cannot process.

### Before you begin

In your `server.xml` file, install and configure the `sipServlet-1.1` feature. For more information, see “Administering Session Initiation Protocol (SIP) on Liberty” on page 1728.

### About this task

The SIP container provides an interface that enables an application to receive all incoming request or response messages that cannot be matched to any existing dialogs. Any request or response messages that are not matched to an existing dialog are known as unmatched messages.

An *unmatched request* is a request that has `To` and `From` tags, but the related dialog is not found in the SIP container because it was never created or this dialog is in the invalidated state. When an incoming unmatched request is received by the SIP container, the container responds with a `481 Call/Transaction Does Not Exist` response, and then forwards the incoming request to the listener class. The incoming

request is forwarded as part of the `UnmatchedRequestEvent` event, which is defined in the `com.ibm.websphere.sip.unmatchedMessages.events` package. The event contains an interface to get the incoming unmatched request and the `ServletContext` related to the application that receives the event. The application can use the `ServletContext` to create new SIP activity. The listener cannot create a response for the received unmatched request or proxy the request. When this condition occurs, an `IllegalStateException` exception occurs in the SIP container.

An *unmatched response* is a response that is received in the SIP container, but the response is not matched to any outgoing requests. Before the SIP container discards the unmatched response, the unmatched response is sent to the `UnmatchedMessageListener` listener as part of the `UnmatchedResponseEvent` event. Similar to the unmatched request, the application gets access to the unmatched response and to the related application `ServletContext`.

If an application has more than one defined `UnmatchedMessageListener` listener, each listener is started independent of each other. If you have more than one application on a single application server and multiple applications have `UnmatchedMessageListener` listeners, all listeners are started in a random order. If one application sends a request to another application on the same server as part of application composition, and the SIP container determines that this request is a request that cannot be handled by the SIP container, then all of the `UnmatchedMessageListener` listeners on that server are activated.

The `UnmatchedMessageListener` API is defined in the `com.ibm.websphere.appserver.api.sipServlet` file in the `com.ibm.websphere.sip.unmatchedMessages` package.

## Procedure

You can use one of the following methods in the application code to access the `UnmatchedMessageListener` API:

- Add the `UnmatchedMessageListener` implementation class explicitly as a listener deployment descriptor element in the `sip.xml` file.

```
<listener>
  <listener-class>com.example.MyTimerListener</listener-class>
</listener>
```

- Use the `@javax.servlet.sip.annotation.SipListener` annotation.

```
@SipListener
public class MySipUnmatchedMessagesListener
    implements UnmatchedMessageListener {
    ....
}
```

## SIP proprietary header fields on Liberty

8.5.5.7

You can create a Session Initiation Protocol (SIP) servlet request that includes proprietary header fields. SIP proprietary header fields enable certain SIP settings to be implemented on a per message basis. SIP settings set at the SIP container level apply to all SIP messages handled by that SIP container.

To include one or more proprietary header fields in a message, set up your SIP servlet request such that it includes one or more `SipServletMessage.setHeader(string_name, string_value)` methods. When the application calls `SipServletRequest.send()` to send the request, the message object that is passed to the SIP stack for transmission includes the propriety header information. The SIP stack then creates a client transaction to send out the request and adjusts the SIP configuration settings for this specific request based on any proprietary header fields that are included in the message object. The stack removes the proprietary header fields before the message is sent out to the network.

## Proprietary header fields used to specify timer values

The following proprietary header fields are available for specifying timer values for a specific message. The application can set multiple timer values in one message instance, but cannot specify multiple values for the same proprietary header field.

### IBM-TransactionTimeout

Use this header field to specify, in milliseconds, the length of the client transaction timeout. This header is equivalent to specifying a value for timer B in INVITE client transactions, and timer F in non-INVITE client transactions.

### IBM-RetransmissionInterval

Use this header field to specify, in milliseconds, the length of the request retransmission interval. This header is equivalent to specifying a value for timer A in INVITE client transactions, and timer E in non-INVITE client transactions.

### IBM-RetransmissionMaxInterval

Use this header field to specify, in milliseconds, the maximum retransmission interval. This header is equivalent to specifying a value for timer T2 in non-INVITE client transactions, and timer B in INVITE client transactions.

## SIP SipServletRequest and SipServletResponse classes on Liberty

8.5.5.7

The `SipServletRequest` and `SipServletResponse` classes are similar to the `HttpServletRequest` and `HttpServletResponse` classes that are used when you develop web applications.

Each class gives you the capability to access the headers in the SIP message and manipulate them. Because of the asynchronous nature of the requests and responses, the `SipServletRequest` class also creates new responses for the requests. When you extend the `doInvite` method, only the `SipServletRequest` class is passed to the method. To send a response to the client, you must call the `createResponse` method on the `Request` object to create a response as shown in the following example:

```
protected void doInvite(SipServletRequest req) throws
    javax.servlet.ServletException, java.io.IOException {

    //send back a provisional Trying response
    SipServletResponse resp = req.createResponse(100);
    resp.send();
}
```

Because of their asynchronous nature, SIP servlets can seem complicated; however, something as simple as the previous code sample sends a response to a client.

The following example shows a more complex SIP servlet. With the following method included in a SIP servlet, the servlet blocks all of the calls that do not come from the *example.com* domain.

```
protected void doInvite(SipServletRequest req) throws
    javax.servlet.ServletException, java.io.IOException {

    //check to make sure that the URI is a SIP URI
    if (req.getFrom().getURI().isSipURI()){
        SipURI uri = (SipURI)req.getFrom().getURI();
        if (!uri.getHost().equals("example.com")) {
            //send forbidden response for calls outside domain
            req.createResponse(SipServletResponse.SC_FORBIDDEN).send();
            return;
        }
    }
    //proxy all other requests on to their original destination
    req.getProxy().proxyTo(req.getRequestURI());
}
```

For more information on these classes, see the SIP Servlet Specification 1.1, JSR 289.

## SIP SipSession and SipApplicationSession classes on Liberty

8.5.5.7

Both the SipSession and SipApplicationSession classes can act as the primary place to store data in applications that are designed for distributed or highly available environments.

The SipSession class is the best representative of a specific point-to-point communication between two entities and is the closest to the HttpSession object. Because historically no proxying or forking existed for the HTTP request in HTTP servlets, the need for something higher than a single point-to-point session did not exist. The SIP users expect the proxying and forking activities that require multiple layers of SIP session management. The SipSession class is the lowest point-to-point layer.

The SipApplicationSession class represents the higher layer of SIP session management. One SipApplicationSession class can own one or more SipSession objects. However, each SipSession class can be related to one SipSession object only. The SipApplicationSession class also supports the attachment of any number of other protocol sessions. Currently, only HTTP sessions are supported by any implementations. The SipApplicationSession class has a getSession method, which takes the requested protocol type as an argument.

In many applications, it can be useful to combine HTTP and SIP. For example, you might use this approach to tie together HTTP and SIP sessions to monitor a phone call or to start a phone call through a rich HTTP graphical user interface.

For more information on these classes, see the SIP Servlet Specification 1.1, JSR 289.

---

## Developing OSGi applications in Liberty

8.5.5.5

8.5.5.7

### About this task

This section includes the OSGi application features that are specific to Liberty. Currently a WebSocket application can be deployed in an OSGi Web Application Bundle on Liberty. For more information on creating an application in an OSGi application on WebSphere Application Server traditional, see [http://www-01.ibm.com/support/knowledgecenter/SSEQTP\\_8.5.5/com.ibm.websphere.wdt.doc/topics/tcrtbundleprj.htm?lang=en](http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.wdt.doc/topics/tcrtbundleprj.htm?lang=en).

For information about developing OSGi applications by using WebSphere Developer Tools, see Developing OSGi applications.

## Enable OSGi Applications with Java EE 7 technologies

8.5.5.6

You can enable OSGi Applications with key Java Platform, Enterprise Edition (Java EE) 7 technologies. WebSphere Application Server Liberty Version 8.5.5.6 and later, is a production ready server certified for Java EE 7 Full Platform.

To achieve zero migrations, new features are created and existing features remain unaltered. For example, when support for servlet 3.1 was added, a servlet-3.1 feature was created, and servlet-3.0 was kept to ensure behavior did not change for an existing server deployment.

In an environment before Java EE 7 support, you were required to configure `blueprint-1.0`, or something that depends on it, to be able to deploy OSGi applications. You then either configured other OSGi-specific features, like `wab-1.0`, or generic ones, like `jpa-2.0`, to get other capabilities.

In a Java EE 7 environment, OSGi configuration is in two steps:

1. Decide you want to deploy OSGi Bundles.
2. Decide what technologies you want to use to implement those OSGi Bundles.

## Telling the server you want to deploy OSGi Bundles

The first step is to add the `osgiBundle-1.0` feature to your `server.xml`:

```
<featureManager>
  <feature>osgiBundle-1.0</feature>
</featureManager>
```

Adding the `osgiBundle-1.0` feature enables OSGi Bundles to be deployed as part of an OSGi application.

## Telling the server what component models you want to use

Rather than having OSGi-specific features, like `wab-1.0`, you now configure the same component models you would for Java EE. This configuration enables the use of servlets in Bundles, for example, Web Application Bundles or Http Whiteboard servlets:

```
<featureManager>
  <feature>osgiBundle-1.0</feature>
  <feature>servlet-3.1</feature>
</featureManager>
```

For more information, see [OSGi Web Application Bundles](#), and [OSGi Http Whiteboard](#).

This server configuration adds the ability to use `jpa-2.1` in a Persistence Bundle:

```
<featureManager>
  <feature>osgiBundle-1.0</feature>
  <feature>servlet-3.1</feature>
  <feature>jpa-2.1</feature>
</featureManager>
```

For more information, see [Accessing data using Java Persistence API](#).

Optionally, you can still include `blueprint-1.0`:

```
<featureManager>
  <feature>osgiBundle-1.0</feature>
  <feature>servlet-3.1</feature>
  <feature>jpa-2.1</feature>
  <feature>blueprint-1.0</feature>
</featureManager>
```

## Which Java EE 7 component models are supported?

You can see the full list of Java EE 7 technologies that are enabled for OSGi applications.

## Enabling integration of OSGi application services



8.5.5.5

Using the `osgiAppIntegration-1.0` feature, the OSGi applications that are available within the same Java virtual machine (JVM) can share their services with each other. To enable communication between the OSGi applications, you must declare the appropriate service headers in the application manifest file,

META-INF/APPLICATION.MF. An application that wants to import services from other applications must include the `Application-ImportService` header, and an application that wants to export services to other applications must include the `Application-ExportService` header. If an application wants to export and import services, then both headers must be used.

## About this task

To enable the `osgiAppIntegration-1.0` feature, you must include the feature in the `server.xml` file. To use the feature, you need to use the appropriate headers, such as the `Application-ImportService` and `Application-ExportService`. For more information, see `Application manifest files`. You must add the `binding:=local` directive in the headers to specify the integration of applications that are within the same JVM. The binding directive is specific only to the `osgiAppIntegration-1.0` Liberty feature.

## Procedure

1. Based on your requirement, add one or both application headers to your `MANIFEST.MF` file as given in the following example:

```
Application-ExportService: com.acme.Foo;binding:=local
Application-ImportService: com.acme.Foo;binding:=local
```

where `com.acme.Foo` is the name of the Java interface or class associated with the OSGi service.

**Note:** You must add the `binding:=local` directive along with the application import and export service headers to allow the applications within the same JVM to communicate with each other.

2. Add the feature in the `server.xml` file.  

```
<feature>osgiAppIntegration-1.0</feature>
```

## Custom blueprint namespace handlers

8.5.5.4

The Blueprint Container specification, introduced in the OSGi Enterprise Specification Release 5, provides a simple and easy programming model for creating dynamic applications in the OSGi environment without adding complexity to the Java code.

For more information about the OSGi Enterprise Release specification, see [OSGi specification download](#).

The Blueprint Container specification defines a Dependency injection framework for OSGi. It is designed to handle the dynamic nature of OSGi, where services can become available and unavailable at any time. The specification is also designed to work with plain old Java objects (POJOs) so that the same objects can be used within and outside the OSGi framework. The Blueprint XML files that define and describe the various components of an application are key to the Blueprint programming model. The specification describes how the components get instantiated and wired together to form a running application. For more information, see [OSGi Blueprint Container Specification](#).

Each blueprint bundle must contain a blueprint XML file in order for the blueprint runtime to process the blueprint component of the bundle. The standard blueprint element is defined by the OSGi blueprint specification, and required in every blueprint xml document. It sets the default document namespace to `http://www.osgi.org/xmlns/blueprint/v1.0.0`, for example:

```
<blueprint xmlns="http://www.osgi.org/xmlns/blueprint/v1.0.0">
```

Other namespaces can be added to the blueprint by using standard XML rules, either as prefixed entries, or directly within the custom XML elements. These namespaces can be added either at the top level or they can be inline with the custom XML elements. If it is valid XML, it is parsed correctly. For example, defined in the top-level blueprint element:

```
<blueprint
  xmlns="http://www.osgi.org/xmlns/blueprint/v1.0.0"
  xmlns:tx="http://aries.apache.org/xmlns/transactions/v1.0.0">
```

For example, inline in a custom element:

```
<transaction method="*" value="Required"
  xmlns:tx="http://aries.apache.org/xmlns/transactions/v1.0.0"/>
```

The Blueprint runtime implementation that is provided by Apache Aries project is used to support Blueprint bundles that are contained in OSGi Applications for Liberty. For more information, see Apache Aries. The Aries Blueprint runtime provides an extension mechanism called namespace handlers. A namespace handler provides a processor for custom blueprint extensions or namespaces. A namespace handler implements the `org.apache.aries.blueprint.NamespaceHandler` interface and must be registered in the OSGi service registry with an associated `osgi.service.blueprint.namespace` service property. This property denotes the namespace URIs this handler can process. For example: `http://aries.apache.org/xmlns/transactions/v1.0.0`. The service property value can either be a single String or URI, or a Collection, or an array of String or URI.

The blueprint runtime parses the blueprint descriptors twice. The first pass is fast, and finds only every namespace that is used by the blueprint bundle. If the blueprint bundle uses a non-standard namespace, then the blueprint container attempts to locate `NamespaceHandler` services in the OSGi service registry for each custom namespace. A `NamespaceHandler` service advertises every xml namespace that it can process by using OSGi service properties. The blueprint runtime does not parse the blueprint xml until `NamespaceHandler` services can be found for every custom namespace that is used in the bundle. Unless `NamespaceHandler` services can be found for every custom namespace, the blueprint container is unable to process the bundle. This result can mean that the blueprint container waits indefinitely if no `NamespaceHandler` exists. If this situation is encountered, then the blueprint container issues a warning to the log. When the blueprint parser begins to parse the blueprint xml files, it parses any standard blueprint elements. When the parser reaches a custom element, the parser calls out to the `NamespaceHandler` that advertised support for the namespace of the custom element. Here, the `NamespaceHandler` has the opportunity to process the information in the custom element, modify the runtime blueprint model, or do any other operation. If there is a typing error in any of the namespace definitions, then the blueprint almost certainly fails to start.

A custom `NamespaceHandler` service can be provided by any bundle that is running in Liberty, including Liberty Feature bundles , and OSGi Applications bundles.

---

## Developing WebSocket applications in Liberty

You can configure Liberty to use the WebSocket protocol to enable applications to communicate by using a full duplex connection.

### About this task

To configure a Liberty server to run an application that is enabled for WebSocket 1.0, you must set the `websocket-1.0` feature for WebSocket 1.0 or the `websocket-1.1` feature for WebSocket 1.1.

**Note:** 8.5.5.7

In addition to the WebSocket API which is defined in JSR 356 (Java API for WebSocket version 1.1), an API was added to the WebSphere implementation which allows a servlet or filter to request that the current HTTP Request be "upgraded" to start a WebSocket session. This new API is documented here:

Interface `WsWsocServerContainer`

WebSocket endpoints can make use of templates to match an endpoint to a URI. URIs that should not map to websocket endpoints, even though they match a websocket template, can also be used by a web application. The distinction between mapping a websocket endpoint to a URI or allowing the URI to be treated as a "non-websocket" HTTP Request, is made by the presence or absence of an "Upgrade" header with a value of "websocket" in the HTTP Request.

For information about developing WebSocket applications by using WebSphere Developer Tools, see [Developing WebSocket applications](#).

## WebSocket



8.5.5.4

WebSocket is a standard protocol that enables a web browser or client application and a web server application to communicate by using one full duplex connection.

HTTP was not designed for long-lived, real-time, full duplex communication between two applications. In many instances, a user's web server application or servlet wants to communicate with a client browser or application in a long-lived, real-time, full duplex conversation. In other words, the two applications want to freely read and write data back and forth. An example of this type of application is one that constantly displays changing currency exchange rates on the web browser of a stock trader. Current solutions that involve existing HTTP technology to accomplish this type of communication are cumbersome and inefficient. HTTP solutions, for constant two-way communication between a browser and a server, mostly consists of either polling or two open HTTP connections that handle one-way traffic only, or both.

WebSocket uses a standard HTTP request-response sequence to establish a connection. When the connection is established, the WebSocket API provides a read and write interface for reading and writing data over the established connection in an asynchronous full duplex manner. WebSocket also provides an interface for asynchronously closing the connection from either side.

Because WebSocket uses a standard HTTP request-response sequence to establish a connection, the connection initiation connects through firewalls and proxies in the same manner as an HTTP connection. WebSocket requires full duplex communication, including simultaneous reads and writes on the same connection. Version 8.5.5.3 and later of the WebSphere web server plug-in support full duplex communication, but other firewalls and proxies might require modification to enable this support. WebSocket can also use SSL for secure connections and transmission of data. This protocol uses SSL in the same way that the HTTP protocol uses SSL.

The Liberty WebSocket feature implements the following specifications:

- The WebSocket Protocol - RFC 6455
- Java API for WebSocket - JSR 356



8.5.5.5

Liberty supports the WebSocket 1.0 and WebSocket 1.1 specifications. Compared to WebSocket 1.0, WebSocket 1.1 supports a more robust way of specifying message handlers.

You can download sample programs that implement the WebSocket protocol from [WASdev.net](#). For a walkthrough of using WebSocket on Liberty, see [WebSocket sample application on WASdev.net](#).

---

## Chapter 10. Deploying applications in Liberty

You can deploy web applications, enterprise applications, and OSGi applications in Liberty. You deploy an application by either dropping the application into a previously-defined dropins directory, or by adding an application entry to the server configuration.

### Before you begin

**Distributed operating systems** You can deploy applications as described in this topic, or as described in “Adding and running an application on Liberty by using developer tools” on page 2141.

This topic assumes that you have not disabled dynamic updates to the runtime configuration, as described in “Controlling dynamic updates” on page 1594.

### About this task

By default, the “dropins” directory is automatically monitored. If you drop an application into this directory, the application is automatically deployed on the server. Similarly, if the application is deleted from the directory, the application is automatically removed from the server. The “dropins” directory can be used for applications that do not require additional configuration, such as security role mapping. If you put your applications in the “dropins” directory, you must not include an entry for the application in the server configuration. Otherwise, the server will try to load the application twice and an error might occur. For applications that are not in the “dropins” directory, you specify the location using an application entry in the server configuration. The location can be on the file system or at a URL.

Your application can be packaged as an archive file, a directory, [8.5.5.4](#) or as a loose application where files are in multiple locations. For more information about loose applications, see “Loose applications” on page 2255.

For applications in the “dropins” directory, the file name and file extension are used by the application monitor to determine the type of application, and to generate the application id and application name. For example, if the archive file or directory is named snoop.war, the application monitor assumes that the application is a web application and that the application id and application name is “snoop”. For configured applications, the application type and name are specified.

For more information about the default directory structure and the properties that are associated with directories (for example `server.config.dir`), see “Liberty:Directory locations and properties” on page 1434.

**Note:** Restrictions apply when using the “dropins” directory in a production environment. See “Versioning is not possible for applications in the “dropins” directory” on page 2336.

### Procedure

- Deploy an application by dropping it into the dropins directory.

For example, using the default directory structure, to deploy an application you drop it into the `${server.config.dir}/dropins` directory (that is, `wlp/usr/servers/server_name/dropins`).

You can deploy your application in any of the following ways:

- Place the archive file with its identifying suffix (`.ear`, `.war`, and so on) directly into the `/dropins` directory. For example, `${server.config.dir}/dropins/myApp.war`
- Extract the archive file into a directory named with the application name and the identifying suffix. For example, `${server.config.dir}/dropins/myApp.war/WEB-INF/...`

- Place the archive file or the extracted archive into a subdirectory named with the identifying suffix. For example, `${server.config.dir}/dropins/war/myApp/WEB-INF/...`
- Deploy an application by adding it to the server configuration file.

Configure the application element in the `server.xml` configuration file. See . You must configure the following attributes for the application:

**id** Must be unique and is used internally by the server.

**name** Must be unique and depending on the application. The value of **name** might be used as the context-root of the application. For more information on how the context-root is set for an application, see “Deploying a web application to Liberty” on page 2155.

**type** Specifies the type of application.

- For web applications, the supported type is **war**.
- For enterprise applications, the supported type is **ear**.

**location**

Specifies the location of the application. It can be an absolute path or a URL which you can download the application from. It can also be the file name of your application (including file extension if any).

If the application is available on the file system, the location can either be the full path name or a simple file name. If the location does not include the full path, the application manager looks for the application in `${server.config.dir}/apps` and `${shared.app.dir}`. If the application is available at a URL, the application manager downloads the application to a temporary folder inside the server work area, then starts the application.

**Note:** The location that you specify for a configured application should not be in the “dropins” directory. If you drop an application into the “dropins” directory, and also specify the location in the `server.xml` file, you are telling the server to deploy the application twice.

In the following two examples, the location is the file system. If the location is a URL, enter the URL in the location field.

```
<osgiApplication location="D:/apps/ImpactEBA.eba"/>
<webApplication location="ImpactWeb.war"/>
```

The second example does not include the full path. In this case, you must put the application in one of the following locations:

- `${server.config.dir}/apps` (that is, *server\_directory/user/servers/server\_name/apps*)
- `${shared.app.dir}` (that is, *liberty\_install\_location/usr/shared/apps*)

You can deploy your application to the file system in either of the following ways:

- Place the archive file with its identifying suffix (`.ear`, `.war`, and so on) directly into the chosen location. For example, *application\_directory\_path/myApp.war*
- Extract the archive file into a subdirectory of the chosen location, named with the application name and the identifying suffix. For example, *application\_directory\_path/myApp.war/WEB-INF/...*

**Note:**

- You must create the server-level apps directory, whereas the shared apps directory is present by default. See “Liberty:Directory locations and properties” on page 1434 for more information about the properties associated with the server directories.
- The **application** element can be set before or after the server has started. If the element is set after the server has started, the changes are picked up dynamically.

-  **8.5.5.6** Deploying Contexts and Dependency (CDI) applications in Liberty

A Liberty server can be used to deploy CDI applications by configuring the server for the CDI 1.2 Liberty feature. See “Configuring Liberty for Contexts and Dependency Injection 1.2” on page 1725 for more information.

Applications that use contexts and dependency injection must have CDI enabled. For the CDI 1.2 Liberty feature, CDI is enabled if either:

- There is a `beans.xml` file with a bean discovery mode of `all`.
- There is no `beans.xml` file or a blank `beans.xml` file and classes with bean defining annotations. In this case, there must be a bean deployment archive.

For more information on the different types of bean deployment archive recognized by the CDI 1.2 feature, see “Contexts and Dependency Injection 1.2 behavior changes” on page 1726.

- Remove an application.

For applications that are included in the server configuration, remove the reference to the application from the `server.xml` file. The application is then automatically removed from the server.

For applications that are deployed to the “dropins” directory, delete the application from the directory. The application is then automatically removed from the server.

To uninstall all applications that are in the “dropins” directory, set the application monitor `dropinsEnabled` property to `false` as described in “Controlling dynamic updates” on page 1594.

## What to do next

For all deployed applications, you can configure whether application monitoring is enabled and how often to check for updates to applications. For the “dropins” directory, you can also configure the name and location of the directory and choose whether to deploy the applications that are in the directory. See “Controlling dynamic updates” on page 1594.

---

## Adding and running an application on Liberty by using developer tools

### Distributed operating systems

You can add applications to the server by right-clicking on the server in the Servers view then selecting Add and Remove from the menu.

### Before you begin

This task assumes that your application is in your Eclipse workspace. If you have a prebuilt application archive file that you want to add and run, you must first import the file into your Eclipse workspace. Alternatively, you can use the steps described in Chapter 10, “Deploying applications in Liberty,” on page 2139.

### About this task

When you add an application to the server, the workbench tries to determine which features are required by the application and enables them in the server configuration for you if they are not already enabled.

### Procedure

1. In the Servers view, right-click the server and select **Add and Remove**.
2. In the **Add and Remove** wizard, under the **Available** list, select the applications you want to add then click **Add**. Or click **Add All** to add all available applications to the server.
3. Alternatively, you can right-click on an application in the **Project Explorer** view and select **Run As > Run on Server**, or **Debug As > Debug on Server**. This adds the application to the server (if not already added), starts the server (if not already started) and runs the application.

## Results

**Tip:** If you are using **Run on Server** or **Debug on Server** and the server is already started, the browser might try to load the application before the server has finished loading it. If this happens, wait for the message in the console view that displays the application has been started and then refresh the browser if necessary.

## Publishing your application by using developer tools

### Distributed operating systems

Publishing involves copying files (projects, resource files, and server configurations) to the correct location for the server to find and use them. You can either publish your application automatically or manually.

### About this task

If you choose to publish your application automatically, the publishing frequency is controlled by a configurable publishing interval. If you do not want to wait for the automatic publishing interval to pass, or the **Never publish automatically** option is enabled, at anytime you can manually request the workbench to issue a publish command to the server. Each manual publish command causes a single publishing request to the server.

### Procedure

- To publish your application to a server automatically, complete the following steps:
  1. Open the Server preferences page by clicking **Window > Preferences > Server > Launching**, and select the **Automatically publish when starting servers** check box. The workbench checks to see if your project and files on the server are synchronized. If they are not, the project and the files are automatically updated when the server is either started or restarted.
  2. (optional) Modify the Publishing settings. To modify the Publishing settings, right-click the server in the Servers view and select **Open**. In the Overview page of the server editor, under the Publishing settings, you will find the following settings:
    - **Never publish automatically:** Specifies the workbench should never publish files to the server.
    - **Automatically publish when resources change:** Specifies the workbench to issue a publish after changes on a file that is associated with the server are saved and a full time interval has passed in the **Publishing interval** setting. In the workbench, the default setting is the **Automatically publish when resources change** option is enabled with a value set in the publishing interval.
    - **Automatically publish after a build event:** Specifies the workbench to issue a publish after changes on a file that requires a build and is associated with the server are saved, and a full time interval has passed in the **Publishing interval** setting.
    - **Publishing interval (in seconds):** Specifies the number of seconds required before the workbench calls a publish to happen on the server. However, if you make a subsequent change to the files before this time interval has completed, the publish is delayed as the timer is reset. The workbench makes a publish to the server only after the full time interval has passed. If you set the publishing interval to 0 seconds, an immediate publish should happen after changes on a file are saved.
- To publish your application to a server manually, complete the following steps:
  1. Select the server and then click the **Publish to the server** icon located on the toolbar.
  2. Right-click the server and then select **Publish**.

## Publishing settings for a WebSphere Application Server Liberty

*Publishing* involves copying files such as application, resource files, and deployment descriptor files to the correct location for the server to find and use them. You can choose whether you want to publish your application on the server or run your application within the development environment without copying the application into the directories of the server.

### About this task

#### Run applications directly from the workspace

The **Run applications directly from the workspace** publishing option requests the server to run your application from the workspace.

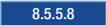
This publishing option publishes faster when an application contains a single root, as opposed to containing multiple roots. The workbench might require additional processing time to publish an application with multiple roots. To determine whether the structure of your application contains a single or multiple roots, use the Project Structure Validator. For details, see *Creating and configuring Java EE projects using wizards*.

#### CAUTION:

**When you are using the Run applications directly from the workspace publishing option, the server can lose track of your application under the following scenarios:**

- If you delete your workspace, the server can no longer find your application. As a result, if you did not put your application under source control management and the workspace is deleted, you can lose your application from your file system.
- If you delete an application from the workspace without removing it from the server, the server can no longer find your application. As a result, you might encounter errors when starting the server because the server tries to start the missing application from the workspace.

### Procedure

1. In the Servers view, double-click your WebSphere Application Server Liberty server to open the server editor.
2. In Liberty Settings, configure publishing settings by choosing any or none of the following options:
  - You can select **Run applications directly from the workspace**.  
This option is selected by default.
  -  You can select **Allow publishing of applications containing errors**.  
If you do not select this option, then when you attempt to publish an application that contains errors, you receive a warning. You can choose to cancel publishing and fix your errors, or you can choose to publish your application without correcting the errors. If you select this option, then you do not receive a warning when you attempt to publish an application that contains errors.
3. Save and close the editor.

## Restart requirements for a modified application on Liberty

When you change an application on Liberty, whether an application or server restart is required depends on whether the Liberty server is started in run mode or debug mode.

### Modifying an application when the server is started in debug mode

In debug mode, some changes require an application restart. For details of which changes require an application restart, use the IBM Rational Application Developer documentation, and see the “Hot Method Replace” section in WebSphere Application Server debug limitations.

If an application restart is required, a Hot Code Replace Failed dialog box is displayed, giving you an option to restart the application. If you click **Yes**, the application is restarted automatically; if you click **No**, you must restart the application manually.

For details on how to start the server in debug mode, use the IBM Rational Application Developer documentation, and see [Debug on server](#).

## Modifying an application when the server is started in run mode

In run mode, most changes require an application restart. If an application restart is required, the application is restarted automatically as part of the application publish operation from the developer tools. Some changes require a server restart.

---

## Customizing automatic feature detection

Control which features are added to each project and resolve feature conflicts.

### About this task

Automatic feature detection selects and enables features that an application needs. However, the automatic process can lead to conflicts among features. Customize automatic feature detection to fit your preferences and resolve conflicts.

### Procedure

1. Right-click the project and select **Properties**.
2. Expand **Liberty** and select **Required Features**.
3. Set the action for each feature to **Always add**, **Prompt before adding**, or **Never add**. **Always add** is the default. See [Disabling automatic feature detection](#) to set the default for all projects or to disable automatic feature detection.
4. Resolve or ignore feature conflicts by using the Feature Conflict dialog box.
  - a. The Feature Conflict dialog box appears when features conflict. New features are marked with **new**.
  - b. Click **Add...** to add a feature, or select a feature and click **Remove** to remove it.
  - c. Click **OK** after you resolve the conflicts.

**Note:** Click **Ignore** to avoid conflict resolution. If conflicts are ignored, the server might not work as expected.

---

## Packaging a Liberty server from the command line

From the command line, you can create a compressed file that contains a Liberty runtime environment, the files in the shared resources directory, a specific server, and the applications that are embedded in the server. You can also choose to exclude the runtime binary files from the compressed file.

### About this task

The Liberty server is lightweight, and therefore you can easily package a server installation in a compressed file. You can store this package, distribute it to colleagues, and then use it to deploy the installation to a different location or to another machine, or even embed the installation in a product distribution.

The server installation that you want to package cannot already be joined to a collective. You can only package a stand-alone server.

**Note:** **Distributed operating systems** The resulting file is created by using UTF-8 encoding for entry names, so the tool that you use to open the file must be able to use UTF-8 encoding for entry names. The `jar` command in a Java SDK uses this format.

## Procedure

To package a Liberty server from the command line, complete the following steps:

1. Open a command line, then change directory to the `wlp/bin` directory.
2. Stop the server.
3. Run the **package** command to create a package.

**8.5.5.5** You can package the Liberty profile server or the runtime.

- Package the Liberty server.

The default archive format is `.zip` on all platforms apart from z/OS where it is `.pax`. You can also generate a `.jar` archive.

If you do not specify a server name, `defaultServer` is used. If you do not specify the **--archive** parameter, the value of `server_name` is used for `package_file_name`, and the compressed file is created in the `${server.output.dir}` directory.

Choose the correct command for your environment.

**Distributed operating systems**

IBM i

Use this command to generate a `.zip` archive.

```
server package server_name --archive=package_file_name.zip --include=all
```

where `package_file_name.zip` is a file name that you choose. This file name can include a full path name. If the full path is omitted, a compressed file called `package_file_name.zip` is created in the `${server.output.dir}` directory.

**Distributed operating systems**

IBM i

Use this command to generate a `.jar` archive. The advantage of a `.jar` archive is that the scripts in the `bin` directory keep their permissions, so they are executable when the package is installed.

```
server package server_name --archive=package_file_name.jar --include=all
```

where `package_file_name.jar` is a file name that you choose.

For more information about extraction options with this archive file, see “Java archive file extraction options” on page 1376.

**z/OS**

Use this command to generate a `.pax` archive.

```
server package server_name --archive=package_file_name.pax --include=all
```

where `package_file_name.pax` is a file name that you choose. This file name can also include a full path. If the full path is omitted, a compressed file called `package_file_name.pax` is created in the `${server.output.dir}` directory.

The pax archive format saves the extended attributes that are required for the Liberty to work as designed in all supported scenarios. If a compressed file in ZIP format is required, specify the target archive name and include the `.zip` extension. If the specified name ends with `.zip`, then a compressed file in ZIP format is generated, instead of the z/OS default PAX format.

An archive format of `.jar` is not valid on z/OS.

You can also use the **--include** option with this command. For example, the `--include=all` option packages the runtime binaries and the relevant files in the `${WLP_USER_DIR}` directory; the `--include=usr` option packages only relevant files in the `${WLP_USER_DIR}` directory, effectively excluding the runtime binaries from the compressed file.

The `--include=usr` option is not valid with an archive format of `.jar`.

#### 8.5.5.0

If you use the `--include=minify` option, the **server** command packages only those parts of the runtime environment, and files in the `${WLP_USER_DIR}` directory, that are required to run the server. This option significantly reduces the size of the resulting archive.

The parts of the runtime environment that are retained by the `minify` operation depend on the features that are configured in the server that you are packaging. Only those features that are required to run the server are retained, and the remaining features are removed. Therefore, you cannot later enable a feature that has been removed. For example, if only the `servlet-3.0` feature is retained, you cannot later enable the `jpa-2.0` feature.

You can repeat the `minify` operation to further reduce the size of the archive if the configuration is changed. There is, however, no reverse operation for the `minify` operation, so if you later require one or more features that have been removed, you must begin again with a complete Liberty server.

While the `minify` operation is running, the server is temporarily started, and you see the associated messages. For this reason, you cannot use the `--include=minify` option with a server that is not able to be started, but you can package it with the `--include=all` or `--include=usr` options.

You can specify the operating systems that you want the packaged server to support by using the `--os` option with the `--include=minify` option.

For example, to package a server with `z/OS` support removed, use the following command:

```
server package --archive="nozoz.zip" --include=minify --os=-z/OS
```

To package a server with `OS/400` support retained, but `z/OS` support removed, use the following command:

```
server package --archive="small.zip" --include=minify --os=OS/400,-z/OS
```

To package a server that supports only Linux, use the following command:

```
server package --archive="linux.zip" --include=minify --os=Linux
```

**Note:** `z/OS` To unpackage a file on `z/OS`, go to the location where you want to unpackage the file and then run the following command. The `-ppx` option is used to preserve the extended attributes.

```
pax -ppx -rf location filename.pax
```

Where *location* is the path where the file exists and *filename.pax* is the name of the file.

- **8.5.5.5** Package the Liberty runtime.

Create a runtime archive that contains the `wlp` directory, but does not contain the `usr` directory. The naming convention for a server package is *package\_name.zip*; for example, `CustomerPortalApp.zip`. To create a runtime archive, run the **package** command without a server name and with the `--include=wlp` option:

```
server package --include=wlp
```

To specify a package file name and target location, add the `--archive=package_path_name` option; for example:

```
server package --include=wlp --archive=c:\temp\myPackage.zip
```

If you do not specify a valid package name or target location with the `--archive` option, then the command creates the `wlp.zip` runtime archive in the `$WLP_OUTPUT_DIR` location, which is the `${wlp.install.dir}/usr/servers` directory by default. The target location must exist before running the command. Thus, if the target location is `c:\temp`, the `C:\temp` directory must exist and have write permission for the command to write the archive to the `C:\temp` directory.

---

## Using JNDI binding for constants from the server configuration files

You can bind constants into the default Java Naming and Directory Interface (JNDI) namespace from the server configuration files by using the `<jndiEntry>` element on Liberty.

## About this task

The default JNDI namespace is available in the Liberty profile to provide bindings to miscellaneous objects required by applications. Any data sources declared in the server configuration files are available in the default JNDI namespace. Additionally, you can bind Java strings and primitive data types in the configuration file into JNDI namespace. These constants are then made available to an application at run time, providing a simple and portable way to pass configuration values into the application.

For more information about the JNDI naming, see Naming.

## Procedure

1. Add a constant into the default JNDI namespace by specifying the `jndi-1.0` Liberty feature in the `server.xml` file of the Liberty server.

```
<featureManager>
  <feature>jndi-1.0</feature>
</featureManager>
```

2. Bind constants into the JNDI namespace by specifying the `<jndiEntry>` elements with **jndiName** and **value** attributes in the `server.xml` file.

```
<jndiEntry jndiName="schoolOfAthens/defaultAdminUserName" value="plato" />
<jndiEntry jndiName="schoolOfAthens/defaultAdminPassword" value="republic" />
```

If you want to bind an instance of `java.net.URL` into the JNDI namespace, use the `jndiURLEntry` configuration:

```
<jndiURLEntry jndiName="urls/IBMKnowledgeCenter" value="http://www-01.ibm.com/support/knowledgecenter/" />
<jndiURLEntry jndiName="urls/WASDevNet" value="http://wasdev.net" />
```

3. Look up the constants from an application by using a JNDI context with the following code:

```
Object jndiConstant = new InitialContext().lookup("schoolOfAthens/defaultAdminUserName");
String defaultAdmin = (String) jndiConstant;
```

### Note:

- The `lookup()` method returns an object to the application. The type of the object is determined by interpreting the value stored in the `jndiEntry` element as a Java literal string or primitive data type. If the parsing fails, the exact value is provided as an unmodified string.
- The `jndiEntry` element supports the integer, floating-point, boolean, character, and string literals as described in Java Language Specification, Java SE 7 Edition, section 3.10. String and character literals might contain unicode escaped sequences (see section 3.3: Unicode Escaped Sequences), and the octal and character escape sequences (see section 3.10.6: Escape Sequences for Character and String Literals). Null literals and class literals are not supported; for more information see section 3.10.7: The null literal and section 15.8.2: Class Literals.

See the following examples of Java literals:

- The string "Hello, world" followed by a newline character:

```
<jndiEntry jndiName="a" value="'Hello, world.\n'" />
```

- The integer with a binary value 1010101:

```
<jndiEntry jndiName="b" value="0b1010101" />
```

- The single character 'X':

```
<jndiEntry jndiName="c" value="'X'" />
```

- The double-precision floating point number 1.0:

```
<jndiEntry jndiName="d" value="1.0D" />
```

For more information about `<jndiEntry>` element, see .

---

## Using JNDI binding for dynamic values from the server configuration files

8.5.5.4

You can bind a reference for dynamic values into the default Java Naming and Directory Interface (JNDI) namespace from the server configuration files by using the `jndiReferenceEntry` element on the Liberty profile.

### About this task

The default JNDI namespace is available in Liberty to provide bindings to miscellaneous objects that are required by applications. Based on the features that are enabled in your server, you can bind a predetermined set of objects to the default JNDI namespace. Additionally, you can bind a reference to an object factory, which dynamically determines the value that it returns. You can also use this object factory to return custom object types to an application.

For more information about the JNDI naming, see [Naming](#).

### Procedure

1. Add the `jndi-1.0` Liberty feature to the `server.xml` file.

```
<featureManager>
  <feature>jndi-1.0</feature>
</featureManager>
```

2. Create an `ObjectFactory` class that returns a programmatically defined value.

```
import javax.naming.spi.ObjectFactory;

public class MyObjectFactory implements ObjectFactory {
    @Override
    public Object getObjectInstance(Object o, Name n, Context c, Hashtable<?, ?> envmt) throws Exception {
        Properties p = new Properties();
        p.put("abc", 123);
        return p;
    }
}
```

3. Include the `ObjectFactory` in a `library` element in the `server.xml` file:

```
<library id="objectFactoryLib">
  <fileset dir="${server.config.dir}/lib" includes="factory.jar"/>
</library>
```

4. Declare the factory in a `jndiObjectFactory` element in the `server.xml` file and reference the previously declared library.

```
<jndiObjectFactory id="objectFactory" libraryRef="objectFactoryLib"
  className="com.ibm.example.factory.MyObjectFactory"/>
```

You can also declare the type of object that the factory returns. The type is returned by the `javax.naming.Context.list()` method.

```
<jndiObjectFactory id="objectFactory" libraryRef="objectFactoryLib"
  className="com.ibm.example.factory.MyObjectFactory"
  objectClassName="java.util.Properties"/>
```

5. Declare the entry in a `jndiReferenceEntry` element in the `server.xml` file and reference the previously declared factory.

```
<jndiReferenceEntry id="refEntry" jndiName="ref/entry" factoryRef="objectFactory"/>
```

6. To declare more properties for the `jndiReferenceEntry` element in the `server.xml` file:

```
<jndiReferenceEntry id="refEntry" jndiName="ref/entry" factoryRef="objectFactory">
  <properties abc="123"/>
</jndiReferenceEntry>
```

These additional properties are represented as `javax.naming.StringRefAddr` on the `javax.naming.Reference` that is passed to the factory:

```
import javax.naming.spi.ObjectFactory;

public class MyObjectFactory implements ObjectFactory {
    @Override
    public Object getObjectInstance(Object o, Name n, Context c, Hashtable<?, ?> envmt) throws Exception {
        Properties p = new Properties();
        Reference ref = (Reference) o;
        RefAddr refAddr = ref.get("abc");
        p.put("abc", refAddr == null ? 123 : refAddr.getContent());
        return p;
    }
}
```

7. You can inject the resulting object to an application by using a resource environment reference:

```
@Resource(name="ref/entry")
private Properties properties;
```

---

## Deploying OSGi applications to Liberty

You can deploy OSGi applications to Liberty by enabling a list of server features in the `server.xml` file.

### About this task

By providing a list of OSGi-specific server features, Liberty provides OSGi support for your applications. These features are as follows:

- `blueprint-1.0`
- `osgi.jpa-1.0`
- `wab-1.0`

For a full list of server features in Liberty, see “Liberty features” on page 826.

## Sharing common OSGi bundles for Liberty

You can share common OSGi bundles by placing them in a directory and configuring the `server.xml` file for your server, so that those common OSGi bundles are available to your OSGi applications.

### Procedure

- Create a directory in your file system and place all the common OSGi bundles into the directory.
- Add the following lines into the `server.xml` file.

```
<bundleRepository>
  <fileset dir="directory_path" include="*.jar"/>
</bundleRepository>
```

Where *directory\_path* is the path to the directory that contains the common OSGi bundles.

- Define a dependency on the common bundle using `import` phrase in the `manifest.mf` file of your OSGi application.

---

## Deploying data access applications to Liberty

Deploying a data access application includes more than installing your web application archive (WAR) or enterprise archive (EAR) file onto Liberty. Deployment can include tasks for configuring the data access resources of the server and overall runtime environment.

## About this task

This following topics are covered in this section:

### Procedure

- Configure a data source and JDBC driver for database connectivity in a Liberty profile
- Deploy an JDBC application to Liberty
- Optional: Configure connection pooling in Liberty
- Optional: Develop an application-defined data source on Liberty
- Optional: Configure transaction recovery for data sources on Liberty
- Migrating data access applications to Liberty

## Deploying an existing JDBC application to Liberty

You can take an existing application that uses Java Database Connectivity (JDBC) and a data source, and deploy the application to a server.

### About this task

You can take an existing JDBC application and deploy it to Liberty. To complete this deployment, you add the `jdbc-4.0` Liberty feature to the `server.xml` file. You must also add code that tells the server the JDBC driver location and specifies properties that the JDBC driver uses to connect to the database.

In this example, you can extend your servlet application, or use the one provided here to test the interactivity that is used through the JDBC driver is working as expected.

### Procedure

1. Create a server.
2. Start the server.
3. Add the `jdbc-4.0` and the `servlet-3.0` Liberty features to the `server.xml` file.

```
<server>
  <featureManager>
    <feature>jdbc-4.0</feature>
    <feature>servlet-3.0</feature>
  </featureManager>
</server>
```

To check that the server is working and that the features are enabled successfully, see the `console.log` file, which is stored in the `logs` directory of the server. You can view it using any text editor. You should see something like this example:

```
[AUDIT ] CWWKF0012I: The server installed the following features: [jdbc-4.0, jndi-1.0].
[AUDIT ] CWWKF0008I: Feature update completed in 0.326 seconds.
```

4. Specify the database type and the data source location in the `server.xml` file.

Where `path_to_derby` is the location where `derby` is installed on your operating system, `lib` is the folder where `derby.jar` is located, and `data/exampleDB` is the directory that is created if it does not exist.

For example:

```
<jdbcDriver id="DerbyEmbedded" libraryRef="DerbyLib"/>

<library id="DerbyLib">
  <fileset dir="C:/path_to_derby/lib" includes="derby.jar"/>
</library>

<dataSource id="ds1" jndiName="jdbc/exampleDS" jdbcDriverRef="DerbyEmbedded">
  <properties.derby.embedded
```

```

        databaseName="C:/path_to_derby/data/exampleDB"
        createDatabase="create"
    />
</dataSource>

```

For information about other options for coding data source definitions, see “Using Ref tags in configuration files” on page 1592.

5. Add some SQL create, read, update, and delete statements to your JDBC application to test the interactivity with the database.

```
package wasdev;
```

```

import java.io.*;
import java.sql.Connection;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.sql.Statement;
import javax.annotation.Resource;
import javax.servlet.*;
import javax.servlet.http.*;
import javax.servlet.annotation.WebServlet;
import javax.sql.DataSource;

```

```
@WebServlet("/HelloWorld")
```

```
public class HelloWorld extends HttpServlet {
```

```
    @Resource(name = "jdbc/exampleDS")
```

```
    private DataSource ds1;
```

```
    private Connection con = null;
```

```
    private static final long serialVersionUID = 1L;
```

```
    public HelloWorld() {
```

```
        super();
```

```
    }
```

```
    public void doGet(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException {
```

```
        response.setContentType("text/html");
```

```
        PrintWriter out = response.getWriter();
```

```
        out.println("<H1>Hello World Liberty</H1>\n");
```

```
        try {
```

```
            con = ds1.getConnection();
```

```
            Statement stmt = null;
```

```
            stmt = con.createStatement();
```

```
            // create a table
```

```
            stmt.executeUpdate("create table cities (name varchar(50) not null primary key, population int, county var");
```

```
            // insert a test record
```

```
            stmt.executeUpdate("insert into cities values ('myHomeCity', 106769, 'myHomeCounty')");
```

```
            // select a record
```

```
            ResultSet result = stmt.executeQuery("select county from cities where name='myHomeCity'"); would result.ne
```

```
            // display the county information for the city.
```

```
            out.println("The county for myHomeCity is " + result.getString(1));
```

```
            // drop the table to clean up and to be able to rerun the test.
```

```
            stmt.executeUpdate("drop table cities");
```

```
        }
```

```
    catch (SQLException e) {
```

```
        e.printStackTrace();
```

```
    }
```

```
    finally {
```

```
        if (con != null){
```

```
            try{
```

```
                con.close();
```

```
            }
```

```
        catch (SQLException e) {
```

```
            e.printStackTrace();
```

```
        }
```

```
    }  
  }  
}
```

## 6. Compile your application.

Where *path\_to\_liberty* is the location you installed Liberty on your operating system, and *path\_to\_app* is the location of the Java file of the application you want to compile.

Example on Windows:

```
C:\> javac -cp  
path_to_liberty\wlp\dev\api\spec\com.ibm.ws.javaee.servlet.3.0_1.0.1.jar  
path_to_App\HelloWorld.java
```

Example on Linux:

```
mo@machine01:~> javac -cp  
path_to_liberty/wlp/dev/api/spec/com.ibm.ws.javaee.servlet.3.0_1.0.1.jar  
path_to_App/HelloWorld.java
```

If the **javac** command is not recognized, ensure that you have the Java bin directory in the PATH environment variable of your operating system.

## 7. Add the application to the server.

In this example, the JDBC application is put in the dropins directory of the server:

```
...\dropins\HelloWorldApp.war\WEB-INF\classes\wasdev\HelloWorld
```

The wasdev directory uses the same package name that is used in HelloWorld.java.

## 8. Check that your JDBC application is working.

For this example, go to this URL:

```
http://localhost:9080/HelloWorldApp/HelloWorld
```

Port 9080 is the default HTTP port that is used by the Liberty server. You can check which HTTP port your server is set on by looking in the server.xml file.

The output on the browser for this example looks like:

```
Hello World Liberty  
The county for myHomeCity is myHomeCounty
```

## Enabling JDBC Tracing for Liberty

JDBC tracing for Liberty is enabled either through a driver-specific custom trace setting, or using the application server supplemental JDBC tracing option.

### About this task

There are two ways of using driver-specific custom trace facilities:

- Using the Java built-in logging mechanism, `java.util.logging`, if the driver supports it.
- Configuring a custom trace setting as a vendor property.

If your JDBC driver does not provide its own custom tracing or logging facilities, or the facilities it provides are minimal, you can use supplemental JDBC tracing from the application server.

If you enable tracing by using either a custom vendor property or supplemental JDBC tracing, you must add the logwriter name to the trace specification in the `bootstrap.properties` file. You can use any of the following logwriters:

**DB2** `com.ibm.ws.db2.logwriter`

**Derby** `com.ibm.ws.derby.logwriter`

**Informix JCC (uses the same driver as DB2)**  
`com.ibm.ws.db2.logwriter`

## Informix JDBC

com.ibm.ws.informix.logwriter

## Microsoft SQL Server JDBC Driver

com.ibm.ws.sqlserver.logwriter

## DataDirect Connect for JDBC for Microsoft SQL Server

com.ibm.ws.sqlserver.logwriter

## Sybase

com.ibm.ws.sybase.logwriter

## Other databases (for example solidDB and MySQL)

com.ibm.ws.database.logwriter

Because changes to trace enablement involve altering the `bootstrap.properties` file, you must restart the server for the changes to take effect.

The following examples illustrate the use of the various JDBC trace methods.

## Procedure

- Use `java.util.logging`.

If the driver you are using supports `java.util.logging`, you can enable it by appending the driver's trace level to `com.ibm.ws.logging.trace.specification` in the `bootstrap.properties` file. See the JDBC vendor documentation for levels and other trace information specific to your driver.

Here is an example for Microsoft SQL Server JDBC Driver:

- Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:com.microsoft.sqlserver.jdbc=FINE
```

Here is an example for Oracle JDBC:

- Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:oracle=FINE
```

- For Oracle, you must also enable the tracing using the system property `oracle.jdbc.Trace`, using one of the following two options:

- In the `bootstrap.properties` file, add the setting `oracle.jdbc.Trace=true`

- In a Java program, add the setting `System.setProperty("oracle.jdbc.Trace", "true");`

- Use custom trace settings.

If the driver you are using has custom trace settings, you set them as JDBC driver vendor properties in the `server.xml` file. You also add the logwriter name to the trace specification in the `bootstrap.properties` file.

Here is an example for DB2 JCC, using the custom property `traceLevel`:

- Example code for the `server.xml` file:

```
<dataSource id="db2" jndiName="jdbc/db2" jdbcDriverRef="DB2Driver" >  
  <properties.db2.jcc databaseName="myDB" traceLevel="-1"/>  
</dataSource>
```

- Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:com.ibm.ws.db2.logwriter=all=enabled
```

Here is an example for Derby Network Client:

- Example code for the `server.xml` file:

```
<dataSource id="derbyNC" jndiName="jdbc/derbyNC" jdbcDriverRef="DerbyNC" >  
  <properties.derby.client databaseName="myDB" createDatabase="create" traceLevel="1"/>  
</dataSource>
```

- Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:com.ibm.ws.derby.logwriter=all=enabled
```

Here is an example for Informix JCC. This database uses the DB2 drivers for JCC connectivity.

– Example code for the `server.xml` file:

```
<dataSource id="informixJCC" jndiName="jdbc/informixJCC" jdbcDriverRef="InformixDriverJCC" >
  <properties.informix.jcc databaseName="myDB" traceLevel="-1"/>
</dataSource>
```

– Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:com.ibm.ws.db2.logwriter=all=enabled
```

- Use supplemental JDBC tracing.

If your JDBC driver does not provide suitable tracing or logging facilities, you can use supplemental JDBC tracing from the application server. The application server automatically determines whether to enable supplemental JDBC tracing, based on the JDBC driver being used. To override this, set the data source property `supplementalJDBCTrace` to true or false.

1. Enable supplemental tracing.

Here is an example for enabling supplemental tracing with the embedded Derby database.

Supplemental JDBC tracing is enabled by default for this database, so you only need to set the logwriter in the `bootstrap.properties` file:

– Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:com.ibm.ws.derby.logwriter=all=enabled
```

Here is an example for enabling supplemental tracing with Informix JDBC. Supplemental JDBC tracing is enabled by default for this database.

– Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:com.ibm.ws.informix.logwriter=all=enabled
```

Here is an example for enabling supplemental tracing, and `java.util.logging`, with Microsoft SQL Server JDBC Driver:

– Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:com.ibm.ws.sqlserver.logwriter=all=enabled:
com.microsoft.sqlserver.jdbc=all
```

Here is an example for enabling supplemental tracing with DataDirect Connect for JDBC for Microsoft SQL Server:

– Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:com.microsoft.sqlserver.jdbc=all
```

Here is an example for enabling supplemental tracing with solidDB. Supplemental JDBC tracing is enabled by default for this database.

– Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:com.ibm.ws.database.logwriter=all=enabled
```

Here is an example for enabling supplemental tracing with Sybase. Supplemental JDBC tracing is enabled by default for this database.

– Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:com.ibm.ws.sybase.logwriter=all=enabled
```

Here is an example for enabling supplemental tracing with other databases:

– Example code for the `bootstrap.properties` file:

```
com.ibm.ws.logging.trace.specification==audit=enabled:com.ibm.ws.database.logwriter=all=enabled
```

2. Disable supplemental tracing

To disable supplemental JDBC tracing, either set the `supplementalJDBCTrace` data source property to false in the `server.xml` file, or remove the logwriter name from the

`com.ibm.ws.logging.trace.specification` property in the `bootstrap.properties` file:

– Example code for the `server.xml` file for solidDB:

```

<dataSource id="soliddb" jndiName="jdbc/soliddb"
    jdbcDriverRef="solidDBDriver" supplementalJDBCTrace="false">
    <properties databaseName="dba" URL="jdbc:solid://localhost:2315/dba/dba" />
</dataSource>

```

- Example code for the bootstrap.properties file for solidDB:  
com.ibm.ws.logging.trace.specification=\*\*audit=enabled

**Note:** If you are not seeing JDBC trace, a feature might be activating JDBC immediately. Check bootstrap.properties and edit it to add JDBC trace specifications.

---

## Deploying a web application to Liberty

By deploying a helloworld.war application, you can learn how server configurations change in Liberty.

### Before you begin

The helloworld.war application uses a simple servlet to display a message on your browser. You can create any other messages to be displayed. The coding of the application is not described within Liberty documents.

### About this task

When you deploy a web application to Liberty by using the developer tools, all configurations that are related to the application are automatically enabled in the server.xml file. However, you can also configure the server.xml file manually by completing the following steps.

This example uses the helloworld.war application and can be accessed by using http://localhost:9090/helloworld. In this example, a Liberty server instance is created, and then its default HTTP port is changed to 9090, and then an application is deployed to it.

### Procedure

1. Create a server named hwserver by using the command `server create hwserver`.
2. Copy the helloworld.war application into the `/usr/servers/hwserver/apps` directory; this directory was created by the `server create` command in step 1.
3. In the server.xml file that was created by the `server create` command, change the default HTTP port of the server hwserver to 9090 by replacing the attribute value `httpPort="9080"` with `httpPort="9090"`:

```

<server description="new server">

    <!-- Enable features -->
    <featureManager>
        <feature>jsp-2.2</feature>
    </featureManager>

    <httpEndpoint id="defaultHttpEndpoint"
        host="localhost"
        httpPort="9090"
        httpsPort="9443" />
</server>

```

4. Configure the application by updating the server.xml in either of the following ways:

- **8.5.5.0** Define the application by using a `webApplication` element:  

```

<server description="Hello World Server">

    <featureManager>
        <feature>servlet-3.0</feature>
    </featureManager>

```

```

<httpEndpoint id="defaultHttpEndpoint" host="*" httpPort="9090" />

<webApplication contextRoot="helloworld" location="helloworld.war" />

</server>

```

- Define the application by using an application element:

```

<server description="Hello World Server">

  <featureManager>
    <feature>servlet-3.0</feature>
  </featureManager>

  <httpEndpoint id="defaultHttpEndpoint" host="*" httpPort="9090" />

  <application context-root="helloworld" type="war" id="helloworld"
    location="helloworld.war" name="helloworld"/>

</server>

```

#### 8.5.5.0

The `webApplication` element can use the same child elements as the `application` element, except for `context-root` and `type`. The two elements do not work together for a `context-root`, and if both an `application` and `webApplication` element define the same `context-root`, only one is used and an error is displayed.

The `context-root` attribute specifies the entry point of the deployed application. The entry point of a deployed application is determined in the following precedence:

- `context-root` in the `server.xml` file
- `application.xml`, if an EAR application
- `ibm-web-ext.xml`, if a web application
- `name` of the application in the `server.xml` file, if a web application
- `Manifest.MF`, if a WAB application
- Directory name or the file name relative to the drop-ins directory of Liberty

**Note:** In an application server `server.xml` configuration, the `application` element can contain a `context-root` tag. This `context-root` tag is applicable in combination with the tag `type="war"`. For all other application types, the `context-root` element has no effect.

It is not possible to override the `context-root` for either an EAR application, or an EBA application. It is only possible to do an override for a stand-alone war file, or `webApplication`.

5. Start the server in foreground by using the command `server run hwserver`.
6. Test the application at `http://localhost:9090/helloworld`.
7. Optional: Stop the server if you don't need it.

---

## Deploying SIP applications to Liberty

#### 8.5.5.7

Session Initiation Protocol (SIP) applications are Java applications that contain at least one SIP servlet. SIP applications are deployed the same way as other web applications.

### Before you begin

Install the `sipServlet-1.1` feature in your Liberty server. For more information, see “Adding and removing Liberty features” on page 1587.

Configure the SIP container. For more information, see “Administering Session Initiation Protocol (SIP) on Liberty” on page 1728.

## About this task

To deploy a SIP application, the application must be packaged in a web archive (WAR) file, a servlet archive (SAR) file, or an enterprise archive (EAR) file that contains a WAR or SAR file.

This task describes how to manually deploy a SIP application. Alternatively, you can deploy a SIP application to Liberty by using the developer tools, which automatically enable all configurations related to the application in the `server.xml` file. For more information, see [WebSphere Developer Tools > Developing > Developing SIP applications](#).

## Procedure

Add your SIP application WAR, SAR, or EAR file to the Liberty server in one of the following ways:

- Move the archive file to the folder for drop-in artifacts in the server configuration directory at `wlp/usr/servers/server_name/dropins`. The Liberty server monitors the `dropins` folder for new applications and automatically installs the application with the default configuration.
- Move the archive file to the folder for applications in the server configuration directory at `wlp/usr/servers/server_name/apps`. Then, install the SIP application in the Liberty server by configuring an `application` element in the `server.xml` file.

The following example installs the `appName.ear` file. The `context-root` attribute specifies the entry point of the deployed application.

```
<application id="appId" name="appName" type="ear" location="appName.ear" context-root="/sip289"/>
```

---

## Deploying a JPA application to Liberty

To enable Liberty to support an application that uses the Java Persistence API (JPA), you add the `jpa-2.0` or `jpa-2.1` feature to the `server.xml` file, depending on which specification level you need. You also need to define persistence contexts and persistence units, and configure access to the entity manager and entity manager factory.

## Before you begin

This task assumes that you have created a Liberty server, on which you want to deploy an application that uses JPA. See “Creating a Liberty server manually” on page 1423.

## About this task

**8.5.5.6** There are two JPA features available in Liberty:

- The `jpa-2.0` feature provides support for applications that use application-managed and container-managed JPA written to the JPA 2.0 specification. The support is built on Apache OpenJPA with extensions to support the container-managed programming model.
- The `jpa-2.1` feature provides support for applications that use application-managed and container-managed JPA written to the JPA 2.1 specification. The support is built on EclipseLink

For information about developing JPA applications by using WebSphere Developer Tools, see [Developing JPA applications](#).

## Procedure

- Add the `jpa-2.0` or `jpa-2.1` feature to the `server.xml` file.
- Add persistence context and persistence unit definitions to the `web.xml` file.

For example:

```
<persistence-context-ref>
  <persistence-context-ref-name>example/em</persistence-context-ref-name>
  <persistence-unit-name>ExamplePersistenceUnit</persistence-unit-name>
</persistence-context-ref>
```

```
<persistence-unit-ref>
  <persistence-unit-ref-name>example/emf</persistence-unit-ref-name>
  <persistence-unit-name>ExamplePersistenceUnit</persistence-unit-name>
</persistence-unit-ref>
```

- Configure access to the entity manager.

For example:

```
Context ctx = new InitialContext();
UserTransaction tran = (UserTransaction) ctx.lookup("java:comp/UserTransaction");
tran.begin();
EntityManager em = (EntityManager) ctx.lookup("java:comp/env/example/em");
Thing thing = new Thing();
em.persist(thing);
tran.commit();
```

- Configure access to the entity manager factory.

For example:

```
Context ctx = new InitialContext();
EntityManagerFactory emf = (EntityManagerFactory) ctx.lookup("java:comp/env/example/emf");
EntityManager em = emf.createEntityManager();
EntityTransaction tx = em.getTransaction();
tx.begin();
Thing thing = new Thing();
em.persist(thing);
tx.commit();
int id = thing.getId();
em.close();
```

## Liberty: Enhancement of JPA entities for JPA 2.0

### 8.5.5.0

The JPA 2.0 specification provider that is included in Liberty is based on Apache OpenJPA. OpenJPA uses Java bytecode enhancement of JPA persistent types (Entity, Embeddable, MappedSuperclass) to add state tracking, and other necessary information to enable persistence and other optimized features within JPA classes. In an application server environment, enhancement of your JPA entities occurs automatically when the application is loaded by the Liberty server.

Pre-enhancement of JPA classes (or build time enhancement) is necessary when a persistence JAR is used in both application server, and non-application server environments. The most common ways to perform build time enhancement are the OpenJPA enhancer Ant task, and PCEnhancer. These build time enhancement options require the OpenJPA library and dependent libraries to be on the classpath. The **wsenhancer** command, in the WebSphere Application Server traditional install, can also be used.

**Note:** The JPA 2.1 specification provider for Liberty is EclipseLink. EclipseLink does not require entity enhancement.

---

## Deploying web services applications to Liberty

By configuring Liberty features in the `server.xml` file, you can deploy web services applications to Liberty.

## Deploying JAX-RS 2.0 applications to Liberty

You can use Java API for RESTful Web Services (JAX-RS) to develop services that follow Representational State Transfer (REST) principles. RESTful services are based on manipulating resources. Resources can contain static or dynamically updated data. By identifying the resources in your application, you can make the service more useful and easier to develop. Liberty provides two Liberty features, `jaxrs-1.1`  and `jaxrs-2.0`, to support the JAX-RS programming model.

8.5.5.6

### Asynchronous processing

You can use the asynchronous processing technique in JAX-RS 2.0 to process threads. Asynchronous processing is supported both in the Client API and in the Server API. For more information about asynchronous processing in Client and Server APIs, see Chapter 8 of JSR 339: JAX-RS 2.0: The Java API for RESTful Web Services (the "Specification").

The following two examples show asynchronous processing in the Client and Server APIs:

- Asynchronous processing in the Client API:

```
Client client = ClientBuilder.newClient();
WebTarget target = client.target("http://example.org/customers/{id}");
target.resolveTemplate("id", 123).request().async().get(
    new InvocationCallbackCustomer() {
        @Override
        public void completed(Customer customer) {
            // Do something
        }
        @Override
        public void failed(Throwable throwable) {
            // Process error
        }
    });
```

- Asynchronous processing in the Server API:

```
@Path("/async")
public class MyResource{

    @GET
    public void getAsync(@Suspended final AsyncResponse asyncResponse){
        CompletionCallback callBack = new CompletionCallback(){
            @Override
            public void onComplete(Throwable throwable) {
                ...
            }
        };
        asyncResponse.register(callBack);
        asyncResponse.resume("some Response");
    }
}
```

The JAX-RS 2.0 implementation in Liberty supports EJB and the use of stateless and singleton session beans as root resource classes. When an EJB method is annotated with `@Asynchronous`, the EJB container automatically allocates the necessary resources for its execution. Thus, in this scenario, it is unnecessary to use an `Executor` to generate an asynchronous response. For example,

```
@Stateless
@Path("/")
class EJBResource {

    @GET @Asynchronous
    public void longRunningOp(@Suspended AsyncResponse ar) {
        executeLongRunningOp();
        ar.resume("Hello async world!");
    }
}
```

Explicit thread management is not needed in this case because that is under the control of the EJB container. The response is produced by calling `resume` on the injected `AsyncResponse`. Hence, the return type of `longRunningOp` is `void`.

## Configuring a resource to receive multipart/form-data parts from an HTML form submission in JAX-RS 2.0

HTML forms that transmit file data must be configured with the `POST` method and the `"multipart/form-data"` action. This data can be received in one of the two ways by the JAX-RS resource method that accepts it with the IBM Java API for RESTful Web Services (JAX-RS) implementation.

### About this task

This task provides instructions for configuring a JAX-RS method to use and produce `multipart/form-data`. The following example illustrates an HTML form:

```
<form action="http://www.example.com/" method="POST" enctype="multipart/form-data">
  <input type="text" name="fileid" />
  <br />
  <input type="text" name="description" />
  <br />
  <input type="file" name="thefile" />
  <br />
  <input type="submit" name="submit" value="submit"/>
</form>
```

You can implement the IBM JAX-RS to receive the data in parts, so you can process these parts yourself, if needed.

### Procedure

Create a resource method. You must declare one of the following resource methods to receive and echo `multipart/form-data` content from an HTTP `POST`:

```
package com.example.jaxrs;
@POST
@Consumes("multipart/form-data")
@Produces("multipart/form-data")

public Response postFormData(IMultipartBody multipartBody) {
    List<IAttachment> attachments = multipartBody.getAllAttachments();
    String formElementValue = null;
    InputStream stream = null;
    for (Iterator<IAttachment> it = attachments.iterator(); it.hasNext(); ) {
        IAttachment attachment = it.next();
        if (attachment == null) {
            continue;
        }
        DataHandler dataHandler = attachment.getDataHandler();
        stream = dataHandler.getInputStream();
        MultivaluedMap<String, String> map = attachment.getHeaders();
        String fileName = null;
        String formElementName = null;
        String[] contentDisposition = map.getFirst("Content-Disposition").split(";");
        for (String tempName : contentDisposition) {
            String[] names = tempName.split("=");
            formElementName = names[1].trim().replaceAll("\\\\", "");
            if ((tempName.trim().startsWith("filename"))) {
                fileName = formElementName;
            }
        }
        if (fileName == null) {
            StringBuffer sb = new StringBuffer();
            BufferedReader br = new BufferedReader(new InputStreamReader(stream));
            String line = null;
            try {
                while ((line = br.readLine()) != null) {
                    sb.append(line);
                }
            } catch (IOException e) {
                e.printStackTrace();
            } finally {
                if (br != null) {
                    try {
                        br.close();
                    } catch (IOException e) {
                        e.printStackTrace();
                    }
                }
            }
        }
    }
}
```

```

        }
        formElementValue = sb.toString();
        System.out.println(formElementName + ":" + formElementValue);
    } else {
        //handle the file as you want
        File tempFile = new File(fileName);
        ...
    }
}
if (stream != null) {
    stream.close();
}
return Response.ok("test").build();
}

```

Or

```

package com.example.jaxrs;
@POST
@Consumes("multipart/form-data")
@Produces("multipart/form-data")

public Response postFormData(List<IAttachment>attachments) {
    List<IAttachment> attachments = multipartBody.getAllAttachments();
    String formElementValue = null;
    InputStream stream = null;
    for (Iterator<IAttachment> it = attachments.iterator(); it.hasNext();) {
        IAttachment attachment = it.next();
        if (attachment == null) {
            continue;
        }
        DataHandler dataHandler = attachment.getDataHandler();
        stream = dataHandler.getInputStream();
        MultivaluedMap<String, String> map = attachment.getHeaders();
        String fileName = null;
        String formElementName = null;
        String[] contentDisposition = map.getFirst("Content-Disposition").split(";");
        for (String tempName : contentDisposition) {
            String[] names = tempName.split("=");
            formElementName = names[1].trim().replaceAll("\\\\", "");
            if ((tempName.trim().startsWith("filename"))) {
                fileName = formElementName;
            }
        }
        if (fileName == null) {
            StringBuffer sb = new StringBuffer();
            BufferedReader br = new BufferedReader(new InputStreamReader(stream));
            String line = null;
            try {
                while ((line = br.readLine()) != null) {
                    sb.append(line);
                }
            } catch (IOException e) {
                e.printStackTrace();
            } finally {
                if (br != null) {
                    try {
                        br.close();
                    } catch (IOException e) {
                        e.printStackTrace();
                    }
                }
            }
            formElementValue = sb.toString();
            System.out.println(formElementName + ":" + formElementValue);
        } else {
            //handle the file as you want
            File tempFile = new File(fileName);
            ...
        }
    }
    if (stream != null) {
        stream.close();
    }
    return Response.ok("test").build();
}

```

The originator of the form POST submission can generate a Content-Transfer-Encoding header for one or more parts of the multipart message. The IBM JAX-RS implementation attempts to auto-decode the payload of the part according to this header when the header is of base64 or quoted-printable encoding type.

## Results

- You have received and echoed data from an HTTP POST with multipart/form-data Content-Type, by allowing the IBM JAX-RS implementation to split and auto-decode the parts for you, and by receiving the still encoded parts to process yourself.

## Configuring JAX-RS 2.0 client



8.5.5.6

For Java API for XML RESTful Web Services 2.0, you can configure the client to access REST endpoints. JAX-RS 2.0 introduces a new and standardized Client API so that you can make HTTP requests to your remote RESTful web services.

### About this task

An instance of `Client` is required to access a Web resource using the Client API. The default instance of `Client` can be obtained by calling `newClient` or `build` on `ClientBuilder`.

### Procedure

1. Enable the `jaxrsClient-2.0` or `jaxrs-2.0` feature in your `server.xml` file:

```
<featureManager>
  <feature>jaxrs-2.0</feature>// If you only need the JAX-RS 2.0 client feature, you can enable jaxrsClient-2.0 instead
</featureManager>
```

2. Create a JAX-RS 2.0 client and send the request to the server:

```
javax.ws.rs.client.ClientBuilder cb = ClientBuilder.newBuilder();

javax.ws.rs.client.Client c = cb.build();
String res = null;

try {
  res = c.target("<Resource_URL>")
    .path("<PATH>")
    .request()
    .get(String.class);
} catch (Exception e) {
  res = "[Error]:" + e.toString();
} finally {
  c.close();
}
```

For more information about the asynchronous JAX-RS 2.0 client, see “Asynchronous processing” on page 2159.

### What to do next

-  **8.5.5.6** Use the `com.ibm.ws.jaxrs.client.timeout` client property to set the timeout value.

```
javax.ws.rs.client.ClientBuilder cb = ClientBuilder.newBuilder();
  cb.property("com.ibm.ws.jaxrs.client.timeout", "1000");
Client c = cb.build();
```

**Tip:** The value of the timeout property is milliseconds, and the type must be long or int. If the type of the value is invalid, the following message is displayed:

CWWKW0700E: The timeout value {0} that you specified in the property `com.ibm.ws.jaxrs.client.timeout` on the JAX-RS Client is invalid.

-  **8.5.5.7** Use the `com.ibm.ws.jaxrs.client.connection.timeout` client property and the `com.ibm.ws.jaxrs.client.receive.timeout` client property to set the timeout values.

- `com.ibm.ws.jaxrs.client.connection.timeout`  

```
javax.ws.rs.client.ClientBuilder cb = ClientBuilder.newBuilder();
    cb.property("com.ibm.ws.jaxrs.client.connection.timeout", "1000");
    Client c = cb.build();
```
- `com.ibm.ws.jaxrs.client.receive.timeout`  

```
javax.ws.rs.client.ClientBuilder cb = ClientBuilder.newBuilder();
    cb.property("com.ibm.ws.jaxrs.client.receive.timeout", "1000");
    Client c = cb.build();
```

**Tip:** The value of the timeout property is millisecond, and the type must be long or int. If the type of the value is invalid, the following message is displayed:

CWWKW0700E: The timeout value {0} that you specified in the property `com.ibm.ws.jaxrs.client.receive.timeout` on the

- Use the following client properties for client proxy support:

```
ClientBuilder cb = ClientBuilder.newBuilder();
cb.property("com.ibm.ws.jaxrs.client.proxy.host", "hostname");
cb.property("com.ibm.ws.jaxrs.client.proxy.port", "8888");
cb.property("com.ibm.ws.jaxrs.client.proxy.type", "HTTP");
```

```
Client c = cb.build();
```

- `com.ibm.ws.jaxrs.client.proxy.host`
- `com.ibm.ws.jaxrs.client.proxy.port`

**Tip:** The type of the proxy server port value must be int. The default value is 80. If the value type is invalid, the following message is displayed:

CWWKW0701E: The proxy server port value {0} that you specified in the property `com.ibm.ws.jaxrs.client.proxy.port` o

- `com.ibm.ws.jaxrs.client.proxy.type`

**Tip:** The value of the proxy server type must be HTTP or SOCKS. The default value is HTTP. If the type of the proxy server is invalid, the following message is displayed:

CWWKW0702E: The proxy server type value {0} that you specified in the property `com.ibm.ws.jaxrs.client.proxy.type` o

- Use the `com.ibm.ws.jaxrs.client.ltpa.handler` client property to set the SSO cookie and set the value to true.

```
ClientBuilder cb = ClientBuilder.newBuilder();
    Client c = cb.build();
    c.property("com.ibm.ws.jaxrs.client.ltpa.handler", "true");
```

If you want to use the Secure Sockets Layer (SSL) function in JAX-RS 2.0, you need to enable the `ssl-1.0` or `appSecurity-2.0` feature. For the LTPA token function, you must enable the `appSecurity-2.0` feature.

For more information about how to configure the environment to run the JAX-RS 2.0 client with SSL through IHS, see [Configuring IBM HTTP server SSL support](#).

**Note:** The `ssl-1.0` feature is a subfeature of the `appSecurity-2.0` feature. If you enable the `jaxrsClient-2.0` feature and the `ssl-1.0` feature, the `appSecurity-2.0` feature is enabled automatically.

- Use the `com.ibm.ws.jaxrs.client.ssl.config` client property to set the SSL reference id of your `server.xml` file.

```
ClientBuilder cb = ClientBuilder.newBuilder();
    cb.property("com.ibm.ws.jaxrs.client.ssl.config", "mySSLRefId");
    Client c = cb.build();
```

For more information about establishing trust by extracting the certificate from the IHS key file and adding it to the Liberty JKS file, see [Create a key database file and certificates needed to authenticate the Web server during an SSL handshake](#).

**Note:** The configuration in the `server.xml` file shows as follows:

```
<ssl id="mySSLRefId" keyStoreRef="clientKeyStore" trustStoreRef="clientTrustStore" />
```

- **8.5.5.9** Use the `com.ibm.ws.jaxrs.client.disableCNCheck` client property to disable the common name check.

```
ClientBuilder cb = ClientBuilder.newBuilder();
cb.property("com.ibm.ws.jaxrs.client.disableCNCheck", true);
```

## Deploying EJB in an EAR file for JAX-RS 2.0



**8.5.5.6**

In Liberty, JAX-RS 2.0 supports EJB JAX-RS in EJB JAR file that must be included in an EAR file.

### Procedure

1. Deploy the new `myearfile.ear` file to Liberty.
2. Use the following URL pattern to access the JAX-RS service:  
`http://<host>:<port>/<context root>/<path of jaxrs resource>`

For example, you can access EJB JAX-RS in `<myejbjaxrs.jar>`:

`http://<host>:<port>/myejbjaxrs/<path of jaxrs resource>`

**Note:** If there are EJB JAX-WS classes in the same EJB-jar and the JAX-WS 2.2 feature is enabled, that means JAX-WS router module also exists, then the default context root should be the short file name of EJB jar+ ".jaxrs" like "myejbjaxrs.jaxrs" for `<myejbjaxrs.jar>`.

### Liberty: Implementation of JAX-RS 2.0 web applications

You can use Java API for RESTful Web Services (JAX-RS) to develop services that follow Representational State Transfer (REST) principles. Using JAX-RS, development of RESTful services is simplified.

JAX-RS is a Java API for developing REST applications quickly. This standard API continues to gain support throughout the Java community. While JAX-RS provides a faster way of developing web

applications than servlets, the primary goal of JAX-RS is to build RESTful services. `jaxrs-1.1` and  **8.5.5.6** `jaxrs-2.0` define a server-side component API to build REST applications. IBM JAX-RS provides an implementation of the JAX-RS (JSR 311) specification.

By using the principles of REST, your business applications can benefit from several advantages. RESTful services are generally simpler to develop and consume. Most RESTful services use well-defined standards for delivery such as HTTP. Because HTTP is a protocol that has RESTful properties, RESTful services gain scalability advantages that enable the service to serve different clients and interoperate with multiple services, while permitting future growth. Additionally, clients for RESTful services generally are not difficult to develop, yielding interoperability advantages because most RESTful services use common data representations such as XML and JSON.

By using JAX-RS technology, REST applications are simpler to develop, simpler to consume, and simpler to scale when compared to other types of distributed systems. Many popular and widely used Internet services have successfully provided RESTful APIs to their applications. Third parties have used various REST APIs to build their own businesses and applications.

JAX-RS capabilities are provided by the use of a servlet or a filter. When you configure the `web.xml` file of your web application and assemble the IBM JAX-RS implementation that is based on the Apache Wink framework into the library directory of your web application, your business application is now ready to use JAX-RS capabilities.

For more information, see

- Define the resources in JAX-RS web applications
- Configure the JAX-RS application

- Assemble JAX-RS web applications
- Deploy JAX-RS web applications

**Note:** The context root value in Liberty is either the name of the web module, or the user-defined context root found in the EAR file.

## Liberty: Implementation of secure JAX-RS 2.0 applications

The JAX-RS 1.1 runtime environment from IBM is driven by a servlet derived from the Apache Wink

project.  **8.5.5.6** The JAX-RS 2.0 runtime environment is driven by a servlet derived from the Apache CXF 3.0.2. Within the WebSphere Application Server environment, the lifecycle of servlets is managed in the web container. Therefore, the security services offered by the web container are applicable to REST resources that are deployed in WebSphere Application Server.

You can define and add security constraints on the REST resources using the same tools that is used to assemble REST applications. These constraints are captured in the J2EE web deployment descriptor that is associated with your application. The following list describes security definitions that you can include in the deployment descriptor:

- User authentication when invoking REST resources embodied in the application, including
  - HTTP basic authentication.
  - Form login authentication.
- Authorization control over REST resources as defined by the URL patterns for the resources.
- Use of SSL for transport when invoking REST resources.
- Programmatic use of the SecurityContext object to determine user identity and roles.

All the security mechanisms supported by the web container are applicable to REST resources, including the use of the Kerberos-based SPNEGO authentication mechanism.

For more information, see:

- Securing JAX-RS applications within the web container
- Securing JAX-RS resources using annotations
- Securing downstream JAX-RS resources

**Note:** In Liberty, the default context root is the name of the WAR file. For more information about options when configuring context roots, see “Deploying a web application to Liberty” on page 2155.

### Securing downstream JAX-RS resources:

You can secure downstream Java API for RESTful Web Services (JAX-RS) resources by configuring the BasicAuth method for authentication and by using the LTPA JAX-RS security handler to take advantage of single sign-on for user authentication.

### Before you begin

This task assumes that you have completed the following steps:

- You have installed your JAX-RS application onto the application server.
- You have enabled security for your JAX-RS application.
- You have secured your JAX-RS applications within the web container by configuring downstream JAX-RS applications to use the basic authentication (BasicAuth) method for user authentication.

### About this task

When composing JAX-RS resources, a new LTPA JAX-RS security handler can be used to seamlessly authenticate on downstream resource invocations.

When invoking downstream secure JAX-RS resources, the calling application is required to authenticate to the target resource. If the target resource on a downstream server uses the BasicAuth method for security, the calling application can take advantage of single sign-on (SSO) for JAX-RS resources. Using single sign-on, an authenticated context is propagated along downstream calls. You can use the LTPA-based security client handler to authenticate to downstream resources that are distributed across servers.

To illustrate this scenario, assume that you have two servers in your cell and that you have deployed JAX-RS resources on both of these servers. Suppose from one resource on server1 you need to invoke another resource that is deployed on server2. When server2 resources are secured using the BasicAuth method for authentication, use the LTPA JAX-RS security handler to take advantage of single sign-on and seamlessly propagate user authentication on downstream calls without having to provide or manage user identities and passwords in the application.

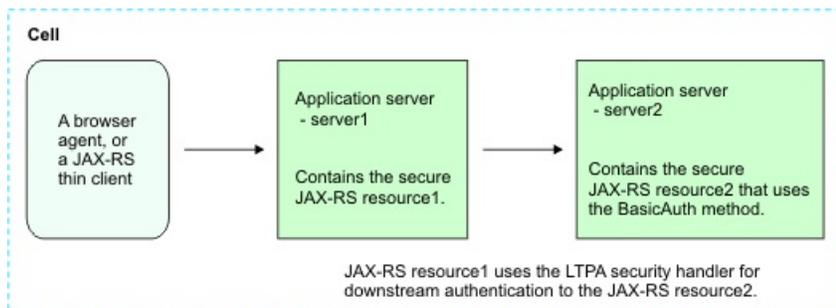


Figure 29. Securing JAX-RS downstream resources

Use the following steps to configure user authentication to a downstream server using the JAX-RS security handler at application build time.

### Procedure

- At application build time, use the LTPA-based security client handler, `LtpaAuthSecurityHandler`, to authenticate to downstream resources that are distributed across servers.
  - For JAX-RS 1.1, when using the `LtpaAuthSecurityHandler` class, ensure that you target resources using the `https` scheme for your URLs, and that the target application is SSL-enabled. It is highly recommended to use SSL connections when sending user credentials, including LTPA cookies. You may explicitly turn off the requirement for SSL in the `LtpaAuthSecurityHandler` class by invoking the `setSSLRequired` method on the security handler with the `false` value. The default value is `true`.

```
yourLtpaAuthSecHandler.setSSLRequired(false);
```

-  **8.5.5.6** For JAX-RS 2.0, you can use the `com.ibm.ws.jaxrs.client.ltpa.handler` client property to set SSO cookie and set the value to `true`:

```
ClientBuilder cb = ClientBuilder.newBuilder();
```

```

Client c = cb.build();
c.property("com.ibm.ws.jaxrs.client.ltpa.handler", "true");
WebTarget t = c.target("http://" + serverIP + ":" + serverPort + "/" + moduleName + "/ComplexClientTest/ComplexReso
String res = t.path("echo1").path("test1").request().get(String.class);
c.close();
ret.append(res);
  
```

-  **8.5.5.6** If you want to use the Secure Sockets Layer (SSL) function in JAX-RS 2.0, you need to enable the `ssl-1.0` or `appSecurity-2.0` feature. For the LTPA token function, the `appSecurity-2.0` feature is must.

**Note:** The `ssl-1.0` feature is a subfeature of the `appSecurity-2.0` feature. If you enable the `jaxrsClient-2.0` feature and the `ssl-1.0` feature, the `appSecurity-2.0` feature is enabled automatically.

- Add the security handler to the handlers chain.

3. Create the REST client instance.
4. Create the resource instance that you want to interact with.
5. Substitute a value representing your resource address.

## Results

You have defined secure JAX-RS resources such that when downstream resources are invoked, you can use single sign-on and seamlessly propagate user authentication on downstream calls without having to provide or manage user identities and passwords in the application.

## Example

For JAX-RS 1.1, the following code snippet demonstrates how to use this security handler that is packaged as part of the JAX-RS client.

```
import org.apache.wink.client.Resource;
import org.apache.wink.client.RestClient;
import org.apache.wink.client.ClientConfig;
import org.apache.wink.client.handlers.LtpaAuthSecurityHandler;

ClientConfig config = new ClientConfig();
LtpaAuthSecurityHandler secHandler = new LtpaAuthSecurityHandler();

// Add this security handler to the handlers chain.
config.handlers(secHandler);

// Create the REST client instance.
RestClient client = new RestClient(config);

// Create the resource instance that you want to interact with.
// Substitute a value representing your resource address
resource =
    client.resource("http://localhost:8080/path/to/resource");

// Now you are ready to begin calling your resource.
```



8.5.5.6

For JAX-RS 2.0, the following code snippet demonstrates how to use this security handler that is packaged as part of the JAX-RS client.

```
ClientBuilder cb = ClientBuilder.newBuilder();
Client c = cb.build();
c.property("com.ibm.ws.jaxrs.client.ltpa.handler", "true");

String res = "";
res = c.target("http://" + serverIP + ":" + serverPort + "/" + moduleName + "/rest/ltpa")
    .request()

c.close();
return res;
```

## JAX-RS 2.0 behavior changes



8.5.5.6

The JAX-RS 2.0 implementation contains some behavior changes. These changes might cause applications to behave differently or fail on JAX-RS 2.0 if the applications are upgraded from JAX-RS 1.1.

The following list describes the differences between JAX-RS 1.1 and JAX-RS 2.0:

- In JAX-RS 1.1 and Jersey, if an EJB or CDI class creates a new instance that is returned by the JAX-RS `application.getSingletons()` method, the engine uses the returned instance and does not try to access the instance from the EJB or CDI container. In JAX-RS 2.0, for the same scenario, the engine tries to access

the instance from the EJB or CDI container. If the instance can be accessed, the retrieved instance is used. But if the instance cannot be accessed, the returned instance from the `getSingletons()` method is used. For example:

```
@Override
public SetObject getSingletons() {
    SetObject objs = new HashSetObject();
    objs.add(new CDIInjectResource());
    objs.add(new EJBInjectResource());
    return objs;
}
```

- | • JAX-RS 2.0 includes many API changes when it handles the MultiPart file. For example, in JAX-RS 1.1, the `@FormParam` can be used to handle the MultiPart file, but in JAX-RS 2.0, only `@IMultipartBody` or `@IAttachment` can be used to handle the MultiPart file. For more information, see [Configuring a resource to receive multipart/form-data parts from an HTML form submission in JAX-RS 2.0](#).
- | • The jackson packages that are displayed as a third-party API in JAX-RS 1.1 are no longer displayed in JAX-RS 2.0. If you want to use any `org.codehaus.jackson` APIs in your application, you need to compress the jackson packages in your application.
- | • If you specify `javax.ws.rs.core.Application` for the servlet name in the `web.xml` file, the `getClasses` method in the Application object, which is injected by `@Context`, does not return the resource classes.

```
<servlet>
  <servlet-name>javax.ws.rs.core.Application</servlet-name>
</servlet>
<servlet-mapping>
  <servlet-name>javax.ws.rs.core.Application</servlet-name>
  <url-pattern>/*</url-pattern>
</servlet-mapping>
```

- The JAX-RS 2.0 specification states that a provider is a class that implements one or more JAX-RS interfaces and that can be annotated with `@Provider` for automatic discovery. In the scenario, a class has `@Local` annotation that refers to a provider interface, but it does not implement any POJO provider interface, and then it is an invalid provider. For example:

```
@Stateless
@Local(OneLocalInterfaceMyOtherStuffMessageBodyWriter.class)
public class OneLocalInterfaceMyOtherStuffProvide
```

- If you use the `MessageBodyReader` and `MessageBodyWriter` `@Consumes` and `@Produces` annotations, some supported media types might be restricted. Use the `isReadable` method or `isWriteable` method to check the media type. For example:

```
@Provider
@Consumes("<custom/type>")
@Produces("<custom/type>")
@Singleton
public class MyMessageBodyReaderAndWriter implements MessageBodyReader,MessageBodyWriter {

    public boolean isReadable(Class<?> type,
                             Type genericType,
                             Annotation[] annotations,
                             MediaType mediaType) {
        if (mediaType.toString().equals("<custom/type>"))
            return true;
        return false;
    }

    public boolean isWriteable(Class<?> type,
                              Type genericType,
                              Annotation[] annotations,
                              MediaType mediaType) {
        if (mediaType.toString().equals("<custom/type>"))
            return true;
    }
}
```

```

        return false;
    }
    ...
}

```

- You can use asynchronous processing in JAX-RS 2.0 to process threads. For more information, see “Asynchronous processing” on page 2159.
- None of the Wink APIs that are displayed as third-party APIs in JAX-RS 1.1 are supported in JAX-RS 2.0. Here is a partial list:

- `org.apache.wink.common.model.atom.AtomEntry`. For more information about integrating JAX-RS 2.0 with Atom, see “JAX-RS 2.0 integration with Atom” on page 2170.
- `org.apache.wink.client.handlers.BasicAuthSecurityHandler`. If you want to use basic authentication in JAX-RS 2.0, see the following code snippets:

1. Use `ClientRequestFilter` through the JAX-RS 2.0 standard Client API as shown in the code example:

```

import java.io.IOException;
import java.io.UnsupportedEncodingException;
import javax.ws.rs.client.ClientRequestContext;
import javax.ws.rs.client.ClientRequestFilter;
import javax.ws.rs.core.MultivaluedMap;
import javax.xml.bind.DatatypeConverter;

public class BasicAuthFilter implements ClientRequestFilter {

    private final String usr;
    private final String pwd;

    public BasicAuthFilter(String usr, String pwd) {
        this.usr = user;
        this.pwd = pwd;
    }

    public void filter(ClientRequestContext requestContext) throws IOException {
        MultivaluedMap<String, Object> headers = requestContext.getHeaders();

        String token = this.usr + ":" + this.pwd;
        final String basicAuthentication = "Basic " + DatatypeConverter.printBase64Binary(token.getBytes("UTF-8"));
        headers.add("Authorization", basicAuthentication);
    }
}

```

2. Register to the `ClientBuilder`:

```

ClientBuilder cb = ClientBuilder.newBuilder();
cb.register(new BasicAuthFilter("user","password"));

```

- `org.apache.wink.client.handlers.LtpaAuthSecurityHandler`. If you want to use the LTPA-based security client to secure downstream resources, see “Securing downstream JAX-RS resources” on page 2165.
- `org.apache.wink.server.internal.providers.exception.EJBAccessExceptionHandler`. This API is no longer supported because it is the Wink-specified `ExceptionHandler`. You can define your own `ExceptionHandler` to map the `EJBAccessException`.
- `com.ibm.websphere.jaxrs.server.IBMRestFilter`. This API is no longer supported because it is based on Wink Filter.

**Note:** Detect if there are wink jar packages in your application. If there are any wink packages in your application, you must do the following steps:

1. Make sure that there is `Application` subclass defined.
2. At least one of `getClasses` and `getSingletons` must not return null.

- For more information about the supported client properties that can be used in the JAX-RS 2.0 client, see [Configuring JAX-RS 2.0 client](#).

- If you want to use the Secure Sockets Layer (SSL) function in JAX-RS 2.0, do the following steps:
  1. Enable either the `ssl-1.0` feature or the `appSecurity-2.0` feature. For the LTPA token function, the `appSecurity-2.0` feature is required.

**Note:** The `ssl-1.0` feature is a sub-feature of the `appSecurity-2.0` feature. If you enable the `jaxrsClient-2.0` feature and the `ssl-1.0` feature, the `appSecurity-2.0` feature is automatically enabled.

2. Enable the `com.ibm.ws.jaxrs.client.ssl.config` property in the JAX-RS 2.0 client code as follows:

```
ClientBuilder cb = ClientBuilder.newBuilder();
Client c = cb.build();
c.property("com.ibm.ws.jaxrs.client.ssl.config", "mySSLConfig"); //mySSLConfig is the ssl ref id in Liberty server.xml
```

**Note:** This property can bind the Liberty SSL configuration to scopes of `ClientBuilder`, `Client`, and `WebTarget`.

- If you want to use the Wink Client in the JAX-RS 2.0 server run time, do the following steps:
  1. Download the following files that can enable Wink Client in the JAX-RS 2.0 server run time.
    - Download the Apache Wink and related JAR files from <http://wink.apache.org/downloads.html>.
    - Download the Apache HTTP and related JAR files from <http://hc.apache.org/>.

**Note:** If the JAX-RS 2.0 feature is not enabled, you must also download and add the JAX-RS API to the third-party lib. Download the JAX-RS API from <https://jax-rs-spec.java.net/nonav/>.

2. Save all JAR files into the `<third-party lib>` directory.
3. Add the location of `<third-party lib>` to the `server.xml` file:

```
<library id="thirdPartyLib">
  <fileset dir=" <third-party lib>" includes="*.jar" scanInterval="5s"/>
</library>
<enterpriseApplication id="<Your Ear ID>" location="<Your Ear Name>" name="<Your Ear Name>">
  <classloader commonLibraryRef="thirdPartyLib"/>
</enterpriseApplication>
```

**Note:** For more information about asynchronous processing in Client and Server APIs, see Chapter 8 of JSR 339: JAX-RS 2.0: The Java API for RESTful Web Services (the "Specification").

## JAX-RS 2.0 integration with Atom

8.5.5.8

JAX-RS 2.0 can use Apache Abdera to add Atom support.

You can register the following Apache Abdera-based providers with a JAX-RS endpoint and use resource methods to explicitly deal with Abdera Feed or Entry classes:

- Apache Abdera-based Feed provider: `net.wasdev.wlp.sample.abdera.jaxrs.atom.AtomFeedProvider`
- Apache Abdera-based Entry provider: `net.wasdev.wlp.sample.abdera.jaxrs.atom.AtomEntryProvider`

**Note:** Both `AtomFeedProvider` and `AtomEntryProvider` support a formatted Output property.

Now the JAX-RS 2.0 sample on GitHub supports both Maven and Gradle. The online instruction on GitHub also shows you how to use commands or WebSphere Development Tools (WDT) for Eclipse to build or test Liberty sample. For more information, see <https://github.com/WASdev/sample.abdera.jaxrs>.

**Note:** Apache CXF offers you other ways of integrating JAX-RS 2.0 with Atom. For more information, see <https://cxf.apache.org/docs/jax-rs-data-bindings.html#JAX-RSDataBindings-Atom>.

## JAX-RS 2.0 integration with EJB and CDI



8.5.5.6

JAX-RS 2.0 in Liberty integrates with Enterprise JavaBeans (EJB) and Contexts and Dependency Injection (CDI).

For JAX-RS 2.0 to work with enterprise beans, you need to use `@Path` to annotate the class of a bean and convert it to a root resource class.

By integrating with EJB, you can annotate the EJB beans to expose them as REST endpoints. You can also use the JTA and security functions of EJB. JAX-RS 2.0 in Liberty supports the use of stateless and singleton session beans as root resource classes, providers, and application subclasses. By integrating with CDI, you can annotate CDI beans or Managed beans as REST endpoints and use CDI injection for web services. JAX-RS 2.0 in Liberty supports CDI-style beans as root resource classes, providers, and application subclasses. Providers and application subclasses must be singletons or use the application scope. CDI specification makes it easier to integrate Java EE components of different types. It provides a common mechanism to inject component such as EJB components or Managed beans into other components such as JSPs or other EJBs.

For EJB, you can use annotation with stateless session beans and singleton POJO beans.

- For a stateless session bean, use the `@Stateless` annotation as is shown in the following example:

```
@Stateless
@Path("stateless-bean")
public class StatelessResource {...}
```

- For a singleton bean, use the `@Singleton` annotation as is shown in the following example:

```
@Singleton
@Path("singleton-bean")
public class SingletonResource {...}
```

For CDI, you can use the `@ApplicationScoped` and `@Inject` annotations with application scoped beans.

**Tip:** If the CDI feature is disabled, JAX-RS reports no errors, but the instances are obtained by using POJO.

```
@ApplicationScoped
@Path("/ApplicationScopedResource")
public class ApplicationScopedResource {

    private @Inject
    SimpleBean injected;

    ...
}
```

### Restrictions on JAX-RS 2.0 with EJB and CDI

See the following items for the restrictions of JAX-RS 2.0 in Liberty:

- If you use EJB as JAX-RS resource, provider or application, you cannot use the `@Context` injection on constructor of the EJB bean. The reason is that the EJB with default constructor can only be used for JAX-RS according to EJB and JAX-RS specification.
- If you use EJB or CDI annotation in a Java class, but the Liberty feature for EJB (such as `ejbLite-3.2`) or CDI (such as `cdi-1.0`) is not configured in the `server.xml` file, which means there are no EJB or CDI supports in Liberty run time, then the JAX-RS 2.0 engine uses the Java class as POJO class.
- For an Application class, if it implements no interface or it has `@LocalBean` annotation, it is seen as EJB; if it implements local or POJO interfaces, it is not seen as EJB.

- For a Provider:
  - If a class implements POJO provider interfaces only without the `@Local` annotation, it is seen as a valid EJB provider.
  - If a class has the `@LocalBean` annotation and it implements the POJO provider interface, then it is seen as a valid EJB provider.
  - If a class has the local interface with the `@Local` annotation, the local interface is a provider interface. If this class implements the provider interface, then it is a valid EJB provider.
  - If a class has a local interface with `@Local` annotation, and if the local interface is not a provider interface, then it is not a valid provider.  
The reason is that in this case, EJB container can generate EJB stub for the local interface only rather than the POJO provider interface.
  - If a class has the `@Local` annotation only that refers a provider interface, but it does not implement this provider interface, then it is not a valid provider according to the JAX-RS 2.0 specification: A provider is a class that implements one or more JAX-RS interfaces that are introduced in this specification and that might be annotated with `@Provider` for automatic discovery.
- For Resource:
  - If EJB-based resource does not implement any interface, all of the methods that are declared in this class are available as JAX-RS resources.
  - If EJB-based resource implements one interface (local or POJO), then all the methods that are declared in this interface are available as JAX-RS resources.
  - If EJB-based resource implements multiple interface,
    1. If all the interfaces are POJO interfaces without the `@Local` annotation, then all the methods that are declared in interface are available as JAX-RS resources.
    2. If all the interfaces are local interfaces with the `@Local` annotation, then all the methods that are declared in the interface are available as JAX-RS resources.
    3. If some of the interfaces are local interfaces with the `@Local` annotation while others are not local interfaces, then only the methods declared in the local interfaces are available as JAX-RS resources. The reason is that the EJB container can generate EJB stub for local interfaces only in this scenario.
    4. If the EJB-based resource has the `@LocalBean` annotation, then all the methods that are declared in class are available as JAX-RS resource.
    5. If EJB-based resource implements an interface, then JAX-RS resource method must be declared in the interface. If the interface is a provider that can't be modified, then you must create a new interface for the resource class to add the resource method. Otherwise, it is not seen as EJB resource.
  - If a resource class with the `@Path` annotation implements JAX-RS provider interface or it declares with the `@Provider` annotation, this class works as both a resource and a provider. In this case, by default, the JAX-RS 2.0 engine uses only one instance of this class that is shared by the resource and the provider, and the lifecycle of the instance is singleton.
  - If a class is registered in both the `getClasses` and `getSingletons` methods of the application class, then by default, the JAX-RS 2.0 engine uses the instance from the `getSingletons` method and ignore the registration in the `getClasses` method.
  - If a RESTful resource is also a CDI managed bean and its scope is `javax.enterprise.context.Dependent`, the `PreDestroy` method cannot be called because of the CDI restriction.

## JAX-RS 2.0 bean and EJB bean lifecycle

JAX-RS bean and EJB bean have different lifecycle. If the bean lifecycle of JAX-RS and EJB conflicts, the lifecycle is managed by EJB container in Liberty. So the EJB instance is applied while the JAX-RS lifecycle does not work. For more information, see the following table:

Table 171. JAX-RS 2.0 bean and EJB bean lifecycle

Application	JAX-RS 2.0	EJB	Result
Resource	perRequest	Stateless	Stateless
	perRequest	Singleton	Singleton
	Singleton	Stateless	Stateless
	Singleton	Singleton	Singleton
Provider	Singleton	Stateless	Stateless
	Singleton	Singleton	Singleton

## JAX-RS 2.0 scope and CDI scope lifecycle

Beans have a scope that determines the lifecycle of its instances. JAX-RS and CDI have slightly different scopes. If the cope lifecycle of JAX-RS and CDI conflict, see the following table for the result:

Table 172. JAX-RS 2.0 scope and CDI scope lifecycle

Application	JAX-RS 2.0 Scope	CDI Scope annotation	Result
Resource	perRequest	@ApplicationScoped	Singleton
	perRequest	@RequestScoped	perRequest
	perRequest	@Dependent	perRequest
	perRequest	@SessionScoped	Session
	perRequest		perRequest
	Singleton	@ApplicationScoped	Singleton
	Singleton	@RequestScoped	perRequest
	Singleton	@Dependent	Singleton
	Singleton	@SessionScoped	Session
	Singleton		Singleton
Provider	Singleton	@ApplicationScoped	Singleton
	Singleton	@RequestScoped	Singleton
	Singleton	@Dependent	Singleton
	Singleton	@SessionScoped	Singleton
	Singleton		Singleton

## JAX-RS 2.0 scope and CDI scope lifecycle conflict messages

The following warning messages are displayed when the scope lifecycle of JAX-RS 2.0 and CDI conflicts. They are warning messages and no actions are required.

- 

CWWKW1001W: The scope {1} of JAXRS-2.0 Resource {0} does not match the CDI scope {2}. Liberty gets resource instance f

This message is displayed if the JAXRS-2.0 resource scope does not match the CDI scope and the resource instance exists in CDI, so Liberty gets the resource instance from CDI. Instance does not include CDI injection if it is from JAXRS.

- CWWKW1002W: The CDI scope of JAXRS-2.0 Provider {0} is {1}. Liberty gets the provider instance from {2}.

This message is displayed because provider instance is Singleton only. Liberty gets provider instance from CDI if the CDI scope of provider is Dependent or ApplicationScoped. Instance does not include CDI injection if it is from JAXRS.

## JAX-RS 2.0 integration with managed beans

8.5.5.8

JAX-RS 2.0 in Liberty supports the use of managed beans as root resource classes, providers, and application subclasses.

- To integrate JAX-RS 2.0 with managed beans, add the `<feature>managedBeans-1.0</feature>` entry inside the `featureManager` element in the `server.xml` file.
- To use a managed bean as a JAX-RS resource, provider, or application, use the `@ManagedBean` to annotate these classes.

For example, use the Interceptors managed bean feature as follows:

```
@ManagedBean ("JaxrsManagedBean" )
@Path ("/managedbean" )
public class ManagedBeanResource {

    public static class MyInterceptor {
        @AroundInvoke
        public Object around(InvocationContext ctx) throws Exception {
            System. out .println("around() called" );
            return ctx.proceed();
        }
    }

    @GET
    @Produces( "text/plain")
    @Interceptors(MyInterceptor. class )
    public String getIt() {
        return "Hi managed bean!" ;
    }
}
```

## Restrictions on JAX-RS 2.0 with managed beans

Resource injection is only supported by the following JAX-RS component classes that are managed by Contexts and Dependency Injection (CDI):

- Application subclasses
- Providers
- Root resource classes

Specifically, to inject a managed bean instance into a certain JAX-RS component class, you must ensure that this component class can be recognized and managed as a CDI bean.

For example, to inject the `printMyName` managed bean instance into a JAX-RS root resource class as follows, you must add an empty `beans.xml` file in the `.WAR` file/`WEB-INF` repository:

```
@Path ("/managedbean" )
public class ManagedBeanResource {

    @Resource(name = "printMyName" )
    private PrintMyName printMyName ;
}
```

```

@GET
@Produces( "text/plain")
public String getIt() {
    printMyName .print();
    return "Hi managed bean!" ;
}
}

@ManagedBean ("printmyname" )
public class PrintMyName {

    public void print() {
        // TODO Auto-generated method stub
        System. out .println("Injection of ManagedBean is successful" );
    }

}

```

## Sending multiple query parameters from Client - Cascaded or Iterated programming



8.5.5.6

You can see the following sample if you want to send multiple query parameters from the client side to the server.

### About this task

**Note:** Normally, the way to put multiple query parameters in a WebTarget object is by using the following cascaded programming mode:

```
javax.ws.rs.core.Response response = client.target(...).queryParam(key, value).queryParam(key, value).queryParam(key, value);
```

However, in some cases, the cascaded programming mode does not apply because the number of key value pairs is flexible and cannot be predicated. For these cases, you can use the following iteration based programming mode:

```

Map<String, String> queryStrings;
...
javax.ws.rs.client.WebTarget target = client.target(...);
for (String key: queryStrings.keySet()){
    String value = queryStrings.get(key);
    target = target.queryParam(key, value); //It is important to know queryParam method won't update current WebTarget object
}
}
javax.ws.rs.core.Response response = target.request().get();

```

## Using JAX-RS 2.0 context objects to obtain more information about requests



8.5.5.6

Java API for RESTful Web Services (JAX-RS) 2.0 provides different types of context to application subclasses, root resource classes, and providers. You can use the @Context annotation to inject context objects such as HttpHeaders, UriInfo, HttpServletRequest into class field or method parameter in application subclasses, root resource classes, and providers.

### About this task

You can use the following context objects that are available to providers (client and server), resource classes (server only), and Application subclasses (server only):

Context object	Type	Description
Application	Class	The instance of the application-supplied <code>Application</code> subclass can be injected into a class field or method parameter using the <code>@Context</code> annotation. Access to the <code>Application</code> subclass instance allows configuration information to be centralized in that class. <b>Note:</b> This <code>Application</code> subclass cannot be injected into the <code>Application</code> subclass itself since this would create a circular dependency.
UriInfo	Interface	The <code>UriInfo</code> interface provides static and dynamic, per-request information, about the components of a request URI.
HttpHeaders	Interface	The <code>HttpHeaders</code> interface provides access to request header information either in map form or via strongly typed convenience methods.
Request	Interface	The <code>Request</code> interface allows a caller to determine the best matching representation variant and to evaluate whether the current state of the resource matches any preconditions in the request.
SecurityContext	Interface	The <code>SecurityContext</code> interface provides access to information about the security context of the current request.
Providers	Interface	The <code>Providers</code> interface allows for lookup of provider instances based on a set of search criteria.
ResourceContext	Interface	The <code>ResourceContext</code> interface provides access to instantiation and initialization of resource or subresource classes in the default per-request scope.
Configuration	Interface	Both the client and the server runtime configurations are available for injection via <code>@Context</code> . These configurations are available for injection in providers (client or server) and resource classes (server only).

## WADL2JAVA command



8.5.5.6

The **wadl2java** command line tool processes an existing Web Application Description Language (WADL) file and generates the required artifacts for developing Java API for RESTful Web Services (JAX-RS) web service applications. The **wadl2java** command line tool supports the top-down approach to developing JAX-RS web services. When you start with an existing WADL file, use the `wadl2java` command line tool to generate the required JAX-RS artifacts.

## Web Application Description Language (WADL)

WADL is a resource-centric description language that is designed to facilitate the modeling, description, and testing of RESTful web applications. For more information, see Web Application Description Language.

### Syntax

The command syntax is as follows:

```
wadl2java --[options]
```

```
wadl2java -wadlns wadl-namespace -p package-name -sp [schema-namespace =]package-name -tMap schema-type=java-t
```

### Parameters

The following *options* values are available for the **wadl2java** command:

- wadlns** *wadl-namespace*  
Specify the WADL namespace.
- p** *package-name*  
Specifies the Java package name to use for the generated code that represents WADL resource elements.
- sp** [*schema-namespace =*]*package-name*  
Specifies the Java package name to use for the generated code that represents WADL grammar elements. Optionally specify a namespace to Java package name mapping.
- tMap** *schema-type=java-type* \*  
Specifies the optional mapping between WADL parameter or representation schema type and custom Java type.
- repMap** *media-type=class-name* \*  
Specifies the optional mapping between a WADL representation with no **wadl:element** attribute and Java class.
- resource** *resource-name*  
Specify the simple class name to use for the generated code code that represents a WADL resource without the id attribute.
- b** *binding-file-name* \*  
Specify external jaxb binding files. Use one **-b** flag for each binding file.
- catalog** *catalog-file-name*  
Specify catalog file to map the imported wadl or schema.
- d** *output-directory*  
Specify the directory into which the code is placed.
- interface**  
Specifies that interface is generated.
- impl** Specifies that a dummy service implementation is generated.
- async** *methodNames* \*  
Specifies a comma-separated list of method names or identifiers that need to support suspended asynchronous invocations.
- generateEnums**  
Specifies that Enum classes can be generated to represent parameters with multiple options.
- inheritResourceParams**  
Specifies that resource-level (path or matrix) parameters can be inherited by child resources.

**-noTypes**

Turns off generating types

**-noVoidForEmptyResponses**

Use JAX-RS Response return type for methods with no response representation.

**-noAddressBinding**

Specifies that the generator might not use the address jaxb binding file to map `wsa:EndpointReferenceType` or `wsa:EndpointReference` to `javax.xml.ws.wsaddressing.W3CEndpointReference`.

**-supportMultipleXmlReps**

Specifies that if a method contains multiple request XML representations then a separate method per every such representation is generated. Do not enable this option when a server-side JAX-RS code is generated. A single method that contains a `javax.xml.transform`. Source input parameter is generated by default such cases.

**-generateResponseIfHeadersSet**

Use JAX-RS Response return type if WADL Response element has 'header' parameters.

**-generateResponseForMethods *methodNames* \***

Specifies a comma-separated list of method names or identifiers that need to have JAXRS Response return type generated.

**-async *methodNames* \***

Specifies a comma-separated list of method names or identifiers that need to support suspended asynchronous invocations.

**-xjc *xjc-argumentsv* \***

Specifies a comma-separated list of arguments that are passed directly to XJC when the JAXB data binding is used. This option causes XJC to load extra plug-ins that augment code generation. For example, to load the `toString(ts)` plug-in that adds a `toString()` method to all generated types the following *arguments* would be used: `-xjc-Xts` A list of available XJC plug-ins can be obtained by using `-xjc-X`.

**-encoding *encoding***

Specifies the charset encoding to use when Java sources are generated.

**-h|-?|-help**

Display detailed information for options.

**-version|-v**

Display the version of the tool.

**-verbose|-V**

Specifies that the generator runs in verbose mode.

**-quiet|-q|-Q**

`-quiet|-q|-Q`

**wadl** `wadl-url`

## Deploying JAX-WS applications to Liberty

8.5.5.0

You can use Java API for XML-based Web Services (JAX-WS) to develop services and deploy your JAX-WS applications to the Liberty profile. The Liberty feature `jaxws-2.2` supports the JAX-WS programming model.

### Customizing web services endpoints

8.5.5.0

You can use the `ibm-ws-bnd.xml` file to customize web services endpoints for server provider and client within your applications.

## Before you begin

The `ibm-ws-bnd.xml` file must be in the `/WEB-INF` directory of a web-based web services application (WAR file), or in the `/META-INF` directory of a EJB-based web service application (JAR file). If the client is running in `clientContainer`, the `ibm-ws-bnd.xml` file must be in the `/META-INF` directory of the JAR file in the client EAR.

## About this task

By configuring the `ibm-ws-bnd.xml` file, you can override the web services address configurations on both the service provider and consumer, export your web services by using a specific URL in your applications that are deployed on Liberty, and import the web services from JAX-WS client applications.

For all available elements that you can configure within the `ibm-ws-bnd.xml` file, see “Liberty:The `ibm-ws-bnd.xml` file” on page 2186.

## Procedure

### 1. Override web services bindings for service providers.

- a. Override the web services endpoint address. In the `webservice-endpoint` element, you can override the endpoint address of a web service endpoint identified by the **port-component-name** attribute. The **address** attribute specifies the relative path to the context root of your application.

```
<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0_0
  version="1.0">
  <!-- 0 to many endpoint descriptions -->
  <webservice-endpoint port-component-name="Hello" address="/hiService" />
</webservices-bnd>
```

- b. Override the context root for EJB based web services. If the web service is an EJB-based web service and defined in an EJB application (JAR archive), the default context root is the EJB jar name. However, you can override the default value using the **context-root** attribute of the `http-publishing` element.

```
<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0_0
  version="1.0">
  <!-- optional http publishing module overrides -->
  <http-publishing context-root="/HiServer" />
</webservices-bnd>
```

**Note:** The **context-root** attribute takes effective only when the web service is an EJB based web service and defined in an EJB jar archive. If the web service is defined in a web application (WAR archive), no matter if it is an EJB based web service, the **context-root** attribute of the `http-publishing` element is ignored, and the context root will always be the context root of the web application.

### 2. Override web services bindings for client applications.

- a. Override the location of the WSDL document. In the `service-ref` element, you can override the WSDL location of a web service reference within a web service client application.

```
<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```

    xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0.x
    version="1.0">
    <service-ref name="services/hello" wsdl-location="http://localhost:9080/HiServer/hiService?wsdl" />
</webservices-bnd>

```

The **wsdl-location** attribute specifies an absolute URI (either HTTP or file protocol), and it can also be a relative URI to the root of the client application. For example:

```

<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0.x
    version="1.0">
    <service-ref name="services/hello" wsdl-location="WEB-INF/wsdl/hiService.wsdl" />
</webservices-bnd>

```

- b. Override the Port Address. In the port element, you can override the address of a port within web service reference in a web service client.

```

<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0.x
    version="1.0">
    <service-ref name="services/hello" wsdl-location="WEB-INF/wsdl/hiService.wsdl">
        <port name="HelloPort" namespace="http://server.ejb.hello.sample.jaxws.ws.ibm.com/"
            address="http://localhost:9080/HiServer/hiService" />
    </service-ref>
</webservices-bnd>

```

The **address** attribute of the port element specifies the absolute URI of a web service port. If the referenced web service only has one port, you can use the **port-address** attribute of the service-ref element. For example:

```

<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0.x
    version="1.0">
    <service-ref name="services/hello"
        port-address="http://localhost:9080/HiServer/hiService" />
</webservices-bnd>

```

**Note:** If the **port-address** attribute of the service-ref element and the **address** attribute of the port element are both specified, the **address** attribute of the port element takes effect.

## Defining web service policy via policy attachment

In Liberty, you can define your web service policy (WS-Policy) within either policy attachment or Web Services Description Language (WSDL) file of a web service application.

### About this task

When WSDL file is not packaged in your application, you can use the policy attachment to configure the WS-Policy for your web service application. Policy attachment feature is often enabled automatically to your web service application package when you enable Java API for XML Web Services (JAX-WS) 2.2 feature. You only need to configure both web services client and provider sides to define the application's WS-Policy Attachment file.

The WS-Policy support is an implementation of the following specifications on the application server.

- WS-Policy is a specification that web services can use XML to advertise their policies on security, quality of service, and for web service consumers to specify their policy requirements. For more information, see Web Services Policy 1.5 - Framework.

- WS-Policy Attachment defines two general-purpose mechanisms for associating policies, as defined in Web Services Policy Framework, with the subjects to which they apply. For more information, see Web Services Policy 1.2 - Attachment.

## Procedure

1. Create `policy-attachments-client.xml` file or `policy-attachments-server.xml` file.

The following example shows you how to define the attributes in `policy-attachments-client.xml` file or `policy-attachments-server.xml` file:

```
<attachments
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsp="http://www.w3.org/ns/ws-policy"
xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:sp13="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200802"
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
<wsp:PolicyAttachment wsdlNamespace="http://tempuri.org/AreaService/">
  <wsp:AppliesTo>
    <wsp:URI>http://tempuri.org/AreaService/#wsdl11.service(AreaService)</wsp:URI>
  </wsp:AppliesTo>
  <wsp:Policy wsu:Id="UsernameTokenwithPasswordHashoverSSL">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:SupportingTokens>
          <wsp:Policy>
            <sp:UsernameToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken" />
            <wsp:Policy>
              <sp:WssUsernameToken10 />
              <sp:HashPassword />
            </wsp:Policy>
          </sp:UsernameToken>
        </wsp:Policy>
      </sp:SupportingTokens>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>
</wsp:PolicyAttachment>
</attachments>
```

There are two ways of binding policy:

- Define web service URL directly by using Endpoint DomainExpression **<wsa:EndpointReference>** as follows.

```
<wsp:AppliesTo>
  <wsa:EndpointReference>
    <wsa:Address>http://localhost:8091/wsatapp/HelloImplService</wsa:Address>
  </wsa:EndpointReference>
</wsp:AppliesTo>
```

- Bind policy by using URI DomainExpression **<wsp:URI>** as follows.

```
<wsp:AppliesTo>
  <wsp:URI>http://server.test.ws.ibm.com/#wsdl11.service(HelloImplService)</wsp:URI>
</wsp:AppliesTo>
```

The following table shows you the WSDL elements and their identifier expressions in the policy attachment file:

Table 173. `<wsp:URI>` Expression list

WSDL Element	Identifier Expression (Omit targetNamespace)
Definitions	<code>wsdl11.definitions()</code>
Message	<code>wsdl11.message(message)</code>
Message/part	<code>wsdl11.messagePart(message / part)</code>
portType	<code>wsdl11.portType(portType)</code>
portType/operation	<code>wsdl11.portTypeOperation(portType/operation)</code>

Table 173. <wsp:URI> Expression list (continued)

WSDL Element	Identifier Expression (Omit targetNamespace)
portType/operation/input	wsdl11.portTypeOperation.input(portType/operation)
portType/operation/output	wsdl11.portTypeOperation.output(portType/operation)
portType/operation/fault	wsdl11.portTypeOperation.fault(portType/operation/fault)
Binding	wsdl11.binding(binding)
Binding/operation	wsdl11.bindingOperation(binding/operation)
Binding/operation/input	wsdl11.bindingOperation.input(binding/operation)
Binding/operation/output	wsdl11.bindingOperation.output(binding/operation)
Binding/operation/fault	wsdl11.bindingOperation.fault(binding/operation/fault)
Service	wsdl11.service(service)
port	wsdl11.port(service/port)

- Put the policy-attachments-client.xml file or policy-attachments-server.xml file into your application's WEB-INF or META-INF folder.
  - Put policy-attachments-client.xml into your application's WEB-INF or META-INF folder for web service client's WS-Policy.
  - Put policy-attachments-server.xml into your application's WEB-INF or META-INF folder for web service provider's WS-Policy.

## Results

You complete to define the WS-Policy via policy attachment without WSDL file packaged in your application.

## Enabling HTTP conduit client properties and user custom properties

8.5.5.0

You can define the HTTP client properties and user custom properties by using the ibm-ws-bnd.xml file for JAX-WS applications on Liberty.

### Before you begin

The ibm-ws-bnd.xml file must be in the /WEB-INF directory of a web-based web services application (WAR file), or in the /META-INF directory of a EJB-based web service application (JAR file). If the client is running in clientContainer, the ibm-ws-bnd.xml file must be in the /META-INF directory of the JAR file in the client EAR.

### About this task

HTTP client properties and user custom properties can be defined by using the service-ref and port elements in the ibm-ws-bnd.xml file for the specific service client or port that is injected by the @WebServiceRef annotation. Properties in the port element override the same properties in the service-ref element.

#### HTTP client properties

The following HTTP client properties are supported in the Liberty profile; these properties must have the prefix **http.conduit.client..** For example: **http.conduit.client.ConnectionTimeout.** These HTTP client properties are valid only when sending or receiving SOAP messages, and they are not applicable when connecting to a WSDL URL.

- ConnectionTimeout**

- **ReceiveTimeout**
- **AsyncExecuteTimeout**
- **AsyncExecuteTimeoutRejection**
- **AutoRedirect**
- **MaxRetransmits**
- **AllowChunking**
- **ChunkingThreshold**
- **Connection**
- **DecoupledEndpoint**
- **ProxyServer**
- **ProxyServerPort**
- **ProxyServerType**
- **NonProxyHosts**

For more information about these properties, see HTTP configuration schema in Apache CXF and Client HTTP Transport (including SSL support) .

### User Custom Properties

Besides the supported HTTP client properties in Liberty, you can define the user custom properties that might be used in your application, and retrieve these properties from the client request context. All attributes defined in the `properties` element will be put into the service client request context.

For all available elements that you can configure within the `ibm-ws-bnd.xml` file, see “Liberty:The `ibm-ws-bnd.xml` file” on page 2186.

### Procedure

1. Configure HTTP conduit properties. The following examples shows how to configure HTTP client properties **ConnectionTimeout** and **ReceiveTimeout** in the `ibm-ws-bnd.xml` file. The following example shows how to apply the HTTP client properties **ConnectionTimeout** and **ReceiveTimeout** for all the ports of the service client injected by using the `@WebServiceRef(name="service/SimpleEchoService")`, and for the port `SimpleEchoPort`, the value of user custom property **vendor** is also applied.

```
<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_1_0
  version="1.0">
  <service-ref name="service/SimpleEchoService">
    <port name="SimpleEchoPort">
      <properties vendor="IBM" />
    </port>
    <properties http.conduit.client.ConnectionTimeout="10000"
      http.conduit.client.ReceiveTimeout="15000" />
  </service-ref>
  ...
</webservices-bnd>
```

2. Then retrieve the properties defined in the `ibm-ws-bnd.xml` file from the request context of the client that is injected by the `@WebServiceRef(name="service/SimpleEchoService")` annotation as follows.

```
@WebServiceRef(name="service/SimpleEchoService")
private EchoService echoService;
...
Echo echo = echoService.getEchoPort();
BindingProvider bp = (BindingProvider)echo;
```

```
String connTimeout = bp.getRequestContext().get("http.conduit.client.ConnectionTimeout").toString();
String recTimeout = bp.getRequestContext().get("http.conduit.client.ReceiveTimeout").toString();
String vendor = bp.getRequestContext().get("vendor").toString();
...
```

## Enforcing adherence to WSDL bindings in JAX-WS web services

### 8.5.5.0

You can add binding extensions in the WSDL document, and then apply the extensions into your applications with JAX-WS support on Liberty.

### About this task

Liberty supports the use of the `wsdl:binding` extension that is required in the JAX-WS 2.2 specification. This topic describes how to define the WSDL extensions, and bind them with the customized extensibility element in Liberty.

### Procedure

1. Define an extensibility element and map it to the user that is defined in the WSDL extension. The following example shows how to bind with the WSDL extension `{http://server.respectbinding.jaxws22/}goodBinding`.

```
@XmlElement(name = "goodBinding", namespace = "http://server.respectbinding.jaxws22/")
public class GoodBindingElement implements ExtensibilityElement, Serializable {
    private String uri;
    private QName elementType = null;
    private Boolean required = null;

    @XmlAttribute(name = "uri")
    public String getUri() {
        return this.uri;
    }

    @Override
    public QName getElementType() {
        return this.elementType;
    }

    @XmlAttribute(name = "required", namespace="http://schemas.xmlsoap.org/wsdl/")
    public Boolean getRequired() {
        return this.required;
    }

    public void setUri(String uri){
        this.uri = uri;
    }

    @Override
    public void setElementType(QName elementType) {
        this.elementType = elementType;
    }

    @Override
    public void setRequired(Boolean required) {
        this.required = required;
    }
}
```

2. Add the `extensions.xml` file into the `/META-INF` directory of your web or EJB application. This file defines where the extensions can be used in the WSDL document. In the following example, an entry to set the `javax.wsdl.Binding` property as the parent type of the `goodBindingElement` class is added in

the extensions.xml file. The entry also means that the extension {http://server.respectbinding.jaxws22/}goodBinding can be only added under the binding element in the WSDL document.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
```

```
<properties>
  <!-- XML Binding -->
  <entry key="org.apache.cxf.bindings.xml-1">javax.wsdl.Binding=jaxws22.respectbinding.server.common.GoodBindingEl
</properties>
```

3. Add the extension {http://server.respectbinding.jaxws22/}goodBinding under the binding element as follows:

```
...
<binding name="EchoPortBinding" type="tns:Echo">
  <soap:binding transport="http://schemas.xmlsoap.org/soap/http" style="document"/>
  <tns:goodBinding wsdl:required="true" uri="http://good/good" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" />
  <operation name="echo">
    <soap:operation soapAction="" />
    <input>
      <soap:body use="literal"/>
    </input>
    <output>
      <soap:body use="literal"/>
    </output>
    <fault name="Exception">
      <soap:fault name="Exception" use="literal"/>
    </fault>
  </operation>
</binding>
...
```

## Liberty:Implementation of JAX-WS client applications

### 8.5.5.0

You can use the Java API for XML-Based Web Services (JAX-WS) client-side programming model support in Liberty.

#### Implementing static JAX-WS web services clients

You can develop static web services clients based on the Web Services for Java Platform, Enterprise Edition (Java EE) specification and the Java API for XML-Based Web Services (JAX-WS) programming model.

For more information, see [Implementing static JAX-WS web services clients](#).

#### Implementing dynamic JAX-WS web services clients

You can develop dynamic web services clients based on the Web Services for Java Platform, Enterprise Edition (Java EE) specification and the Java API for XML-Based Web Services (JAX-WS) programming model.

For more information, see [Implementing dynamic JAX-WS web services clients](#).

#### Running an unmanaged web services JAX-WS client

You can use the Thin Client for JAX-WS with WebSphere Application Server as a standalone client run time in a pure Java SE environment, or in an OSGi environment. If you are running the Thin Client with non-IBM JDK for Liberty, add the `-Dcom.ibm.websphere.thinclient=true` property on the Java launch command line.

For more information, see [Running an unmanaged web services JAX-WS client](#).

#### Running a managed web services JAX-WS client

You can use the `@WebServiceRef` or `@Resource` annotation to inject instances of a JAX-WS service or endpoint, or you can use Java Naming and Directory Interface (JNDI) look up to perform service lookup.

For more information, see managed clients on Implementing static JAX-WS web services clients and Implementing dynamic JAX-WS web services clients.

**Note:** The following sections, and any subtopics, are not relevant to Liberty:

- Set up a development environment for web services
- WebSphere Application Server default directories
- Deploying web services applications onto application servers

For more information about the `jaxws-2.2` feature, see Liberty features.

## Liberty:Implementation of JAX-WS web services applications

8.5.5.0

You can use Java API for XML-Based Web Services (JAX-WS) server-side programming model support in Liberty.

### Implementing web services applications with JAX-WS

When starting from existing JavaBeans or enterprise beans, you can use a bottom-up approach to developing Web services based on the Java API for XML-Based Web Services (JAX-WS) programming model.

For more information, see Implementing web services applications with JAX-WS.

### Implementing web services applications from existing WSDL files with JAX-WS

When starting with an existing Web Services Description Language (WSDL) file, you can use a top-down approach to developing web services based on the Java API for XML-Based Web Services (JAX-WS) programming model.

For more information, see Implementing web services applications from existing WSDL files with JAX-WS.

**Note:** The following sections, and any subtopics, are not relevant to Liberty:

- Set up a development environment for web services
- WebSphere Application Server default directories
- Deploying web services applications onto application servers

For more information about the `jaxws-2.2` feature, see Liberty features.

## Liberty:The `ibm-ws-bnd.xml` file

8.5.5.0

You can customize web services endpoints and configure security settings for both web services providers and web service clients by using the `ibm-ws-bnd.xml` file in Liberty. You must store this file in the `/WEB-INF` directory of your web application or in the `/META-INF` directory of your EJB module.

The `ibm-ws-bnd.xml` file provides the following element hierarchy:

- `<webservices-bnd>`
  - `<webservice-endpoint-properties>`
  - `<webservice-endpoint>`
  - `<properties>`

- <http-publishing>
  - <webservice-security>
- <service-ref>
  - <properties>
  - <port>
    - <properties>

The description of each element in the `ibm-ws-bnd.xml` file is as follows:

### <webservice-endpoint-properties>

This element is used to define the default properties for all the web services endpoints in the same module. Only one `webservice-endpoint-properties` element can be specified for one module. You can specify any name and value pairs that are applicable to web services endpoint as attributes of the `webservice-endpoint-properties` element.

### <webservice-endpoint>

This element is used to specify the binding for a specified service instance. It has the following attributes:

- **port-component-name:** This attribute is required. It is used to specify the name of a port component.
- **address:** This attribute is optional. It is used to specify the overridden address of a service endpoint.

### <http-publishing>

This element is used to specify the publishing configurations when using HTTP protocol for all the web services endpoints. Only one `<http-publishing>` element can be specified in each module. It has the following attribute:

- **context-root:** This attribute is optional. It is used to specify the context root of the EJB module in an EJB-based JAX-WS application.

### <webservice-security>

This element is used to configure role-based authorization for POJO web services and EJB-based web services. It has the following attributes:

- **security-constraint:** This attribute is optional. It is used to associate security constraints with one or more web resource collections, and only works as complementary configuration of the deployment descriptors or annotations in web applications.
- **security-role:** This attribute is optional. It contains the definition of a security role, and only works as complementary configuration of the deployment descriptors or annotations in web applications.
- **login-config:** This attribute is optional. It is used to configure the authentication method and realm name, and takes effect only for the EJB-based web services in a JAR file. If the same attribute is specified in the deployment descriptor file, the value from the deployment descriptor is used. The value of this attribute must be *BASIC* or *CLIENT\_CERT*.

### <service-ref>

This element is used to define the web services reference configurations for a web services client. It has the following attributes:

- **name:** This attribute is required. It is used to specify the name of a web services reference.
- **component-name:** This attribute is optional. It is used to specify the EJB bean name if the service reference is used in an EJB module.

- **port-address**: This attribute is optional. It is used to specify the address of the web services port if the referenced web services has only one port.
- **wsdl-location**: This attribute is optional. It is used to specify the URL of a WSDL to be overridden.

## <port>

This element is used to define port configurations that are associated with the web services reference. Multiple port elements can be defined within a `service-ref` element. It has the following attributes:

- **name**: This attribute is required. It is used to specify the name of the web services port.
- **namespace**: This attribute is optional. It is used to specify the namespace of the web services port. If the **namespace** attribute is present, the binding is applied to the port that has the same name and namespace. Otherwise, the binding is applied to the port that has the same name.
- **address**: This attribute is optional. It is used to specify the address for the web services port. If present, it overrides the value of **port-address** attribute that is defined in the `service-ref` element.
- **username**: This attribute is optional. It is used to specify the user name for the basic authentication.
- **password**: This attribute is optional. It is used to specify the password for the basic authentication. The password can be encoded.
- **ssl-ref**: This attribute is optional. It refers to the `ssl` element that is configured in the `server.xml` file by using the **id** attribute. If the attribute is not specified but the server supports the transport level security by enabling the `ssl-1.0` feature, the service client uses the default SSL configuration of Liberty.
- **key-alias**: This attribute is optional. It is used to specify the alias of client certificate. If the attribute is not specified, and the web service provider supports the client certificate, then the first certificate in the keystore is used as the value of this attribute. The attribute can also override the **clientKeyAlias** attribute that is defined in the `ssl` element of the `server.xml` file.

## <properties>

This element is used to define the properties for a web services endpoint or client. The attributes can be any name and any value.

- For web service clients, you can specify **client.ConnectionTimeout**, **authorization.UserName**, **tlsClientParameters.disableCNcheck** and other attributes.
- For web service endpoint, you could specify **publishedEndpointUrl**, **org.apache.cxf.wsdl.create.imports** and other attributes.

The following example shows the typical configuration of a `ibm-ws-bnd.xml` file:

```
<?xml version="1.0" encoding="UTF-8"?>
<webservices-bnd xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ws-bnd_
  version="1.0">

  <!-- optional Web service endpoint default properties -->
  <webservice-endpoint-properties org.apache.cxf.wsdl.create.imports="true" ... />

  <!-- 0 to many endpoint descriptions -->
  <webservice-endpoint port-component-name="..." address="optional override address">
    <!-- optional Web service endpoint properties -->
    <properties publishedEndpointUrl="http://www.example.com/services/hello"
      org.apache.cxf.wsdl.create.imports="false" />
  </webservice-endpoint>
  ...

  <!-- optional http publishing module overrides -->
  <http-publishing context-root="optional override of module's context root">
    <!-- optional web.xml fragment for security -->
```

```

<webservice-security>
  <!-- SECURITY CONSTRAINTS -->
  <security-constraint>
    <web-resource-collection>
      <web-resource-name>SayHelloServiceName</web-resource-name>
      <url-pattern>/SayHelloService</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <description>SayHelloServiceAuth</description>
      <role-name>group123</role-name>
    </auth-constraint>
    <user-data-constraint>
      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
  </security-constraint>
  <!-- SECURITY CONSTRAINTS -->
  <security-constraint>
    <web-resource-collection>
      <web-resource-name>SecuredSayHelloServiceName</web-resource-name>
      <url-pattern>/Secured*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <description>SecuredSayHelloServiceAuth</description>
      <role-name>group123</role-name>
    </auth-constraint>
    <user-data-constraint>
      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
  </security-constraint>
  <!-- SECURITY ROLES -->
  <security-role id="group123_id">
    <role-name>group123</role-name>
  </security-role>
  <!-- AUTHENTICATION METHOD: Client certificate or basic authentication -->
  <login-config>
    <auth-method>BASIC</auth-method>
  </login-config>
</webservice-security>
</http-publishing>

<!-- 0 to many client refs -->
<service-ref name="services/sayHelloService"
port-address="http://productServer:productPort/context-root/SayHelloService"/>
<service-ref name="services/securedSayHelloService"
port-address="http://productServer:productPort/context-root/SecuredSayHelloService"
wsdl-location="optional override of WSDL document" />
</webservices-bnd>

```

## Liberty: The web services commands

### 8.5.5.0

Liberty provides several command utilities to work with Java Architecture for XML Binding (JAXB) and Java API for XML Web Services (JAX-WS) applications.

### schemagen command for JAXB applications

Generate a schema file from Java classes by using the **schemagen** schema generator tool to create the XML schema. After you have created a mapping between XML schema and Java classes, XML instance documents can be converted to and from Java objects by using the JAXB binding runtime API. The resulting Java classes contain all the necessary information that the JAXB run time requires to parse the

XML for marshaling and unmarshaling. You can use the JAXB classes within JAX-WS applications or the JAXB classes in your non-JAX-WS Java applications for processing XML data.

For more information, see `schemagen` command for JAXB applications.

### **xjc command for JAXB applications**

You can generate fully annotated Java classes from an XML schema file by using the **xjc** command-line tool that is provided by the JAXB schema compiler. Use the **xjc** schema compiler tool to start with an XML schema definition (XSD) to create a set of JavaBeans that map to the elements and types defined in the XSD schema. After you have created a mapping between XML schema and Java classes, you can convert XML instance documents to and from Java objects by using the JAXB binding runtime API. The resulting annotated Java classes contains all the necessary information that the JAXB runtime requires to parse the XML for marshaling and unmarshaling. You can use the resulting JAXB classes within JAX-WS applications or the resulting JAXB classes in your non-JAX-WS Java applications to process XML data.

For more information, see `xjc` command for JAXB applications.

### **wsgen command for JAX-WS applications**

The **wsgen** command-line tool generates the necessary artifacts required by JAX-WS applications when you start with Java code for Web Services programming. When you start with a service endpoint implementation, use the **wsgen** tool to generate the required JAX-WS artifacts.

For more information, see `wsgen` command for JAX-WS applications.

### **wsimport command for JAX-WS applications**

The **wsimport** command-line tool processes an existing Web Services Description Language (WSDL) file and generates the required artifacts for developing JAX-WS web service applications. When you start with an existing WSDL file, use the **wsimport** command-line tool to generate the required JAX-WS artifacts.

**Attention:** If you want to change the package name of the generated classes, include `-p <Expected_Java_Package_Name>` in the **wsimport** command line. After that, do not change Java package name manually.

For more information, see `wsimport` command for JAX-WS applications.

## **Web Services Atomic Transaction in Liberty**

8.5.5.9

Web Services Atomic Transaction (WS-AT) is an OASIS standard. Now it is supported in Liberty. In this section, you can learn how to enable and configure the WS-AT feature in Liberty.

### **Web Services Atomic Transaction overview:**

8.5.5.9

The Web Services Atomic Transaction (WS-AT) support in the application server provides transactional quality of service to the web services environment. Distributed web services applications, and the resources they use, can take part in distributed global transactions. Now WS-AT is also supported in Liberty.

Web services protocols provide standard ways of defining web services applications, and the applications can use it to operate independently of the product, platform, or programming language that is used. The WS-AT support is an implementation of the following specifications on the application server. These

specifications define a set of web services that enable web services applications to participate in global transactions that are distributed across the heterogeneous web services environment.

- WS-AT is a specific coordination type that defines protocols for atomic transactions. Liberty can only use the Web Services Atomic Transaction Version 1.2 specification.
- Web Services Coordination (WS-COOR) specifies a CoordinationContext and a Registration service with which participant web services can enlist to take part in the protocols that are offered by specific coordination types. Liberty can only use the Web Services Coordination Version 1.2 specification.

The WS-AT support is an interoperability protocol that introduces no new programming interfaces for transactional support. Global transaction demarcation is provided by standard enterprise application use of the Java Transaction API (JTA) UserTransaction interface. If an application component that is running under a global transaction makes a web services request, a WS-AT CoordinationContext is implicitly propagated to the target web services, but only if the appropriate application deployment descriptors have been set, as described in the topic about configuring transactional deployment attributes.

If the application server is the system hosting the target endpoint for a web services request that contains a WS-AT Coordination Context, the application server automatically establishes a subordinate JTA transaction in the target run time environment that becomes the transactional context under which the target web services application runs.

The following figure, shows a transaction context shared between two application servers for a web services request that contains a WS-AT CoordinationContext.

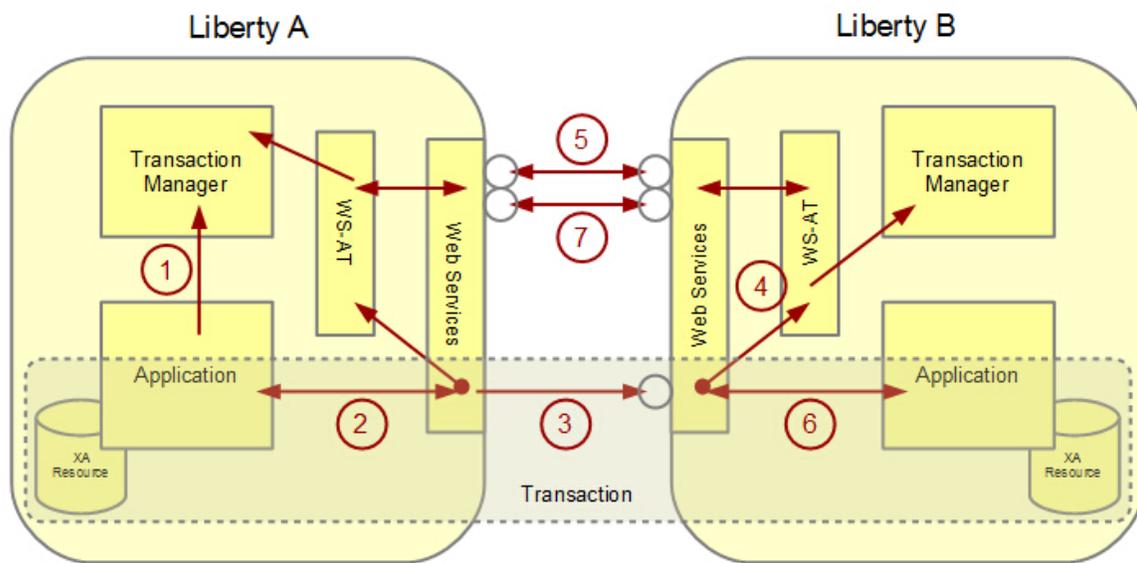


Figure 30. Transaction context shared between two application servers

By default, if you enable WS-AT feature and begin transaction on the client side in Liberty, all the web services operations that are included in client transaction are added to the global transaction. However, if you would run any code outside the scope of the current global transaction, use the UOWManager with type `UOWSynchronizationRegistry.UOW_TYPE_LOCAL_TRANSACTION`. That would have the effect of suspending and resuming the global transaction around that code snippet.

Table 174. Conditions that you can or can not use WS-AT global transaction in Liberty for client outbound

Whether WS-AT feature is enabled	Whether transaction exists	Whether policy assertion exists in WSDL	Whether WS-AT global transaction is enabled
No	No	No	No
No	No	Yes	No with Liberty throwing an exception
No	Yes	No	No
No	Yes	Yes	No with Liberty throwing an exception
Yes	No	No	No
Yes	No	Yes (wsp: Optional="false")	No with Liberty throwing an exception
		Yes (wsp: Optional="true")	No
Yes	Yes	No	Yes
Yes	Yes	Yes	Yes

Table 175. Conditions that you can or can not use WS-AT global transaction in Liberty for server inbound

Whether WS-AT feature is enabled	Whether coordination context exists in SOAP header	Whether policy assertion exists in WSDL	Whether WS-AT global transaction is enabled
No	No	No	No
No	No	Yes	No
No	Yes	No	No with Liberty throwing an exception
No	Yes	Yes	No with Liberty throwing an exception
Yes	No	No	No
Yes	No	Yes (wsp: Optional="false")	No with Liberty throwing an exception
		Yes (wsp: Optional="true")	No
Yes	Yes	No	Yes
Yes	Yes	Yes	Yes

## Application design

WS-AT is a two-phase commit transaction protocol and is suitable for short duration transactions only.

WS-AT is most appropriate for distributing transaction context across web services that are deployed in a single enterprise. Only request-response message exchange patterns carry transaction context because the originator (application or container) of a transaction must be sure that all business tasks that are run under that transaction have finished before requesting the completion of a transaction. Web services called by a one-way request never run under the transaction of the requesting client.

The effect of service faults on WS-AT transactions is similar to the effect of Enterprise JavaBeans (EJB) application exceptions on transactions, as described in the EJB specification. If a service that is running under a requester WS-AT transaction returns a fault, the application server does not automatically mark the transaction rollback-only. The exception handler of the requester chooses whether the transaction can progress and chooses whether to mark the transaction rollback-only. If the requester is running in the application server, the standard JTA or EJB APIs can be used to mark the transaction rollback-only. The

service component that generates the fault might, itself, mark the transaction rollback-only before returning the fault. If the implementation of the service component encounters a system exception, it typically allows its container to handle the exception. Application server containers automatically mark any received transaction context rollback-only when handling a system exception that is generated by a service implementation.

### Configuring Web Services Atomic Transaction: 8.5.5.9

Web Services Atomic Transaction (WS-AT) is an OASIS standard. Now this feature is supported in Liberty.

#### About this task

Before you can configure Web Services Atomic Transaction (WS-AT) in Liberty, you must enable it. This task describes how to enable WS-AT feature in Liberty and also instructs you to add different configurations to WS-AT feature. In addition, you can use the UOWManager with type **UOWSynchronizationRegistry.UOW\_TYPE\_LOCAL\_TRANSACTION** to run any code outside the scope of the current global transaction.

If you do not add the WS-AT feature in Liberty but have any of the following information in your application, an exception message is displayed. The message indicates that the WS-AT feature is not installed in the Liberty log:

- WS-Transaction policy information in WSDL
- Web Services Atomic Transaction Coordination context information in Web Services Soap Header

To enable and configure the WS-AT feature in Liberty, perform the following steps:

#### Procedure

1. To enable the WS-AT feature in Liberty, add the following entry inside the featureManager element in the server.xml file:  

```
<feature>wsAtomicTransaction-1.2</feature>
```
2. Optional: Add some special configurations for the WS-AT feature. You can configure SSL or proxy endpoint for WS-AT internal 2PC protocol communication as follows:  

```
<wsAtomicTransaction SSLEnabled="false" SSLRef="defaultSSLConfig" externalURLPrefix="" clientAuth="false"/>
```

For more information, see Configuring SSL or proxy endpoint parameters in the server.xml file.

3. Optional: To run transactions outside the scope of the current global transaction, add the following code to the client side:

```
UOWManager uowManager = (UOWManager) ctx
    .lookup("java:comp/websphere/UOWManager");
uowManager
    .runUnderUOW(
        UOWSynchronizationRegistry.UOW_TYPE_LOCAL_TRANSACTION,
        false, new UOWAction() {
            public void run() throws Exception {
                ...
                // Example code
                callService1(service1, wsTransactionEnd1);
                ...
            }
        });
```

### Web Services Atomic Transaction security: 8.5.5.9

Web Services Atomic Transaction (WS-AT) defines its own internal web services that are used as part of the protocol. These internal web services are called during the transaction initiation and during the

commitment or rollback processing. Meanwhile WS-AT requires a two-way communication. WS-AT requires a DMZ proxy for Liberty servers to operate in a typical firewall environment and also HTTPS endpoints to get the authorization. The following content describes how to configure proxy and Security Socket Layer (SSL) for WS-AT in Liberty.

## Firewall proxy

When Liberty servers are in a typical firewall environment, the servers cannot communicate with each other through firewalls. In this situation, the servers require a DMZ proxy to operate normally. You can define proxy endpoints by configuring the `server.xml` file.

For example, set IBM HTTP Server (IHS) as the DMZ proxy. In Figure 31, to communicate between two Liberty servers through IHS, perform the following steps:

1. Configure the IHS plug-in to forward requests to Liberty servers. For more information, see [Configuring a web server plug-in for Liberty](#).
  - For IHS 1, configure the IHS 1 plug-in to forward requests to Liberty A and add `<Uri Name="/ibm/wsatservice/*" />` in the `<UriGroup>` item.
  - For IHS 2, configure the IHS 2 plug-in to forward requests to Liberty B and add `<Uri Name="/ibm/wsatservice/*" />` in the `<UriGroup>` item.
2. Add the `externalURLPrefix` parameter to the `server.xml` file in Liberty:
  - In Liberty A, set the `externalURLPrefix` value as `http://proxyserver1:80` for IHS 1 as follows: `<wsAtomicTransaction externalURLPrefix="http://proxyserver1:80"/>`
  - In Liberty B, set the `externalURLPrefix` value as `http://proxyserver2:81` for IHS 2 as follows: `<wsAtomicTransaction externalURLPrefix="http://proxyserver2:81"/>`

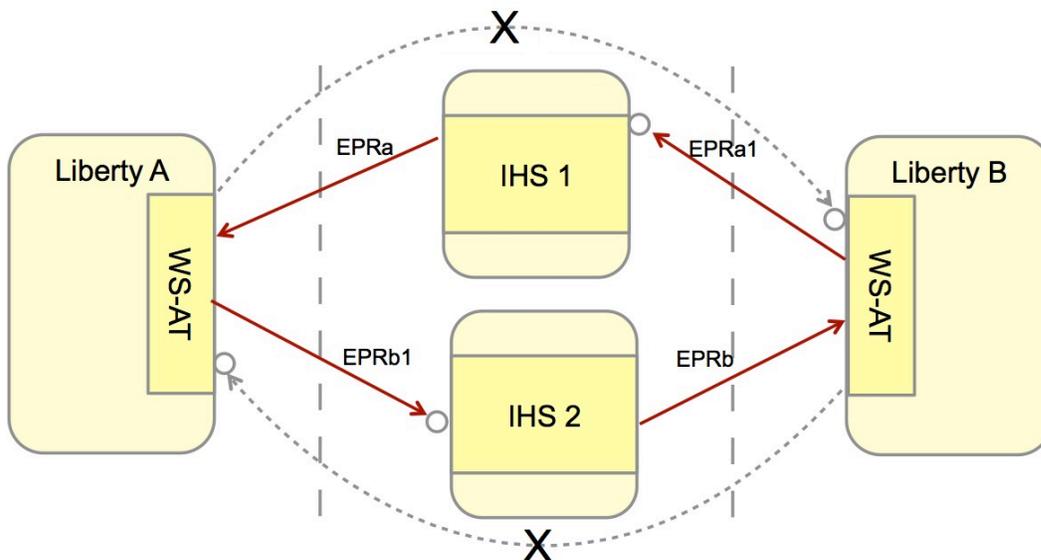


Figure 31. Communication between two Liberty servers through IHS

## Security Socket Layer

By default, Liberty servers communicate without SSL. If you require WS-AT security and security information is redirected to a secure port, you must add the `appSecurity-2.0` Liberty feature to the `server.xml` file. You can also enable SSL in Liberty according to [Securing Liberty and its applications](#).

You can configure SSL for WS-AT security according to the following items:

```
<wsAtomicTransaction SSLEnabled="false" SSLRef="defaultSSLConfig" clientAuth="false"/>
```

Where:

#### **SSLEnabled**

Specifies whether SSL is enabled for WS-AT. Valid values are true and false. The default value is false. Set it to true to enable SSL.

#### **SSLRef**

Defines the SSL configuration in the `server.xml` file. WS-AT requires this SSL configuration to communicate.

#### **clientAuth**

Specifies whether clientAuthentication is enabled for WS-AT. Valid values are true and false. The default value is false. Ensure to set the `clientAuthenticationSupported` value to be true in SSL configuration before you set the `clientAuth` value to be true to enable clientAuthentication.

**Important:** The SSL configuration applies at the Liberty server level only.

**Tip:** In the following code snippet, the default `SSLEnabled` value is false. If you want to enable both SSL and proxy, set the `SSLEnabled` value as true and set the `externalURLPrefix` value as a proxy address that starts with `https://`.

```
<wsAtomicTransaction SSLEnabled="true" SSLRef="defaultSSLConfig" externalURLPrefix="https://proxy" clientAuth="false"/>
```

#### **Web Services Atomic Transaction interoperation:** 8.5.5.9

Liberty supports WS-AT interoperation with WebSphere Application Server classic.

In WebSphere Application Server classic, you can use policy set to control transaction policy. However, if you would run any code outside the scope of the current global transaction in Liberty, use the `UOWManager` with type `UOWSynchronizationRegistry.UOW_TYPE_LOCAL_TRANSACTION`.

If you expect WebSphere Application Server classic to transact with Liberty through proxy, see [Enabling WebSphere Application Server to use an intermediary node for Web services transactions](#).

If you want to use the same Secure Sockets Layer (SSL) to transact between WebSphere Application Server classic and Liberty, see [SSL configurations](#).

---

## Deploying messaging applications to Liberty



8.5.5.6

JMS applications deployed within the Liberty server can make use of the internal embedded messaging provider or the external WebSphere MQ as its JMS messaging provider.

### Deploying JMS applications to connect to the embedded messaging server



8.5.5.6

To deploy messaging applications that use the Java Messaging Service (JMS), you must add the `wasJmsServer-1.0` and `wasJmsClient-2.0` features to the `server.xml` file, and define the connection factory and destination properties. If you want to perform a JNDI lookup, then you must add the `jndi-1.0` feature along with the other two features.

## Before you begin

Ensure that a Liberty server is created on which you want to deploy the messaging application that uses JMS. For more information, see “Creating a Liberty server manually” on page 1423.

**Important:** The `wasJmsClient-2.0` feature supports the features of both JMS 1.1 and JMS 2.0 specifications. However, you can choose to use the `wasJmsClient-1.1` feature if you want to use only the features that are compliant with JMS 1.1 specification.

## About this task

The `wasJmsServer-1.0` feature provides support for applications that use Java Messaging Service 1.1 specifications.

## Procedure

1. Add the `wasJmsServer-1.0`, `wasJmsClient-2.0`, and `jndi-1.0` features to the `server.xml` file.

```
<featureManager>
  <feature>wasJmsServer-1.0</feature>
  <feature>wasJmsClient-2.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>
```

2. Add the destination definitions to the `server.xml` file.

```
<messagingEngine>
  <queue id="QUEUE1"> </queue>
</messagingEngine>
```

3. Optional: Add the `<wasJmsEndpoint>` element to enable the JMS messaging engine to accept the remote incoming messaging connections from TCP/IP (with and without SSL).

```
<wasJmsEndpoint id="InboundJmsEndpoint"
  host="*"
  wasJmsPort="7276"
  wasJmsSSLPort="9100">
</wasJmsEndpoint>
```

**Note:** Adding `<wasJmsEndpoint>` is optional. By default, the Liberty server enables messaging engine to listen on 7276 port (unsecured) and 7286 (secured). If you want to specify a different port, then `<wasJmsEndpoint>` can be configured.

4. Add the connection factory definitions to the `server.xml` file.

- For Point-to-Point domain:

```
<jmsQueueConnectionFactory jndiName="jndi_JMS_BASE_QCF">
  <properties.wasJms
    remoteServerAddress="localhost:7276:BootStrapBasicMessaging" />
</jmsQueueConnectionFactory>
```

```
<jmsQueue jndiName="jndi_INPUT_Q">
  <properties.wasJms queueName="QUEUE1" />
</jmsQueue>
```

- For Publish-Subscribe domain:

```
<jmsTopicConnectionFactory jndiName="eis/tcf">
  <properties.wasJms
    clientID="defaultID" />
</jmsTopicConnectionFactory>
```

```
<jmsTopic jndiName="eis/topic1">
  <properties.wasJms topicName="Football" />
</jmsTopic>
```

The JMS applications are now connected to the embedded messaging server.

# Deploying JMS applications to Liberty to use the IBM MQ messaging provider



8.5.5.6

Through the IBM MQ messaging provider in Liberty, Java Message Service (JMS) messaging applications can use your IBM MQ system as an external provider of JMS messaging resources.

## Before you begin

You must ensure that a Liberty server is created on which you want to deploy the messaging application that uses JMS. For more information, see “Creating a Liberty server manually” on page 1423.

## About this task

The `wmqJmsClient-2.0` feature provides support for applications that use JMS 2.0 specifications.

**Note:** The `wmqJmsClient-2.0` feature supports the features of both JMS 1.1 and JMS 2.0 specifications. However, you can choose to use the `wmqJmsClient-1.1` feature if you want to use only the features that are compliant with JMS 1.1 specification.

## Procedure

1. Add the `wmqJmsClient-2.0` feature to the `server.xml` file. If you want to perform a JNDI lookup, then you must also add the `jndi-1.0` feature.

```
<featureManager>
  <feature>wmqJmsClient-2.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>
```

Adding the `wmqJmsClient-2.0` feature enables the Liberty server to load the necessary IBM MQ bundles that enable you to define the IBM MQ JMS resources. For example, the connection factory and activation specification properties provide client libraries to connect to the IBM MQ network.

2. Specify the location of the WebSphere MQ Resource Adapter by adding the following entry to the `server.xml` file:

```
<variable name="wmqJmsClient.rar.location" value="/path/to/wmq/rar/wmq.jmsra.rar"/>
```

where the `value` attribute specifies the absolute path to the WebSphere MQ Resource Adapter file, `wmq.jmsra.rar`.

For details of the supported versions and obtaining the `wmq.jmsra.rar` file, refer to the WebSphere MQ technote 1633761. Obtain the `wmq.jmsra.rar` file and install it from Fix central.

3. Add the connection factory definitions to the `server.xml` file.

```
<jmsConnectionFactory jndiName="jms/wmqCF" connectionManagerRef="ConMgr6">
  <properties.wmqJms
    transportType="CLIENT"
    hostName="localhost"
    port="1414"
    channel="SYSTEM.DEF.SVRCONN"
    queueManager="QM1"/>
</jmsConnectionFactory>
<connectionManager id="ConMgr6" maxPoolSize="2"/>

<jmsQueue id="jms/queue1" jndiName="jms/wmqQ1">
  <properties.wmqJms
    baseQueueName="MDBQ"
    baseQueueManagerName="QM1"/>
</jmsQueue>
```

4. Configure JMS applications to connect in the BINDING mode.

To allow the JMS applications to connect by using the shared memories or in BINDING mode to IBM MQ, you must have both Liberty and IBM MQ deployed on the same server. To allow JMS

applications to connect in BINDING mode, use the `nativeLibraryPath` element in the `server.xml` file to specify the location of the IBM MQ native libraries.

```
<wmmqJmsClient nativeLibraryPath="/opt/mqm/java/lib64"/>
```

## Deploying JMS application to connect to the Service Integration Bus running on WebSphere Application Server traditional



8.5.5.6

To deploy the messaging applications that use the Java Messaging Service (JMS) to connect to the messaging engine that is running on WebSphere Application Server traditional, you must add the `wasJmsClient-2.0` and `jndi-1.0` features to the `server.xml` file. If you want to perform a JNDI lookup, then you must add the `jndi-1.0` feature. You must also define the connection factory and destination properties.

### Before you begin

Ensure that you created a Liberty server on which you want to deploy the messaging application that uses JMS. For more information, see “Creating a Liberty server manually” on page 1423.

**Important:** The `wasJmsClient-2.0` feature supports the features of both JMS 1.1 and JMS 2.0 specifications. However, you can choose to use the `wasJmsClient-1.1` feature if you want to use only the features that are compliant with JMS 1.1 specification.

### About this task

The `wasJmsClient-2.0` feature provides support for applications that use Java Messaging Service 1.1 specifications.

### Procedure

- Add the `wasJmsClient-2.0` features to the `server.xml` file.

```
<featureManager>
  <feature>wasJmsClient-2.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>
```

- Add the connection factory definitions to the `server.xml` file.

– For Point-to-Point domain:

```
<jmsQueueConnectionFactory jndiName="jndi_JMS_BASE_QCF">
  <properties.wasJms
    remoteServerAddress="localhost:7276:BootstrapBasicMessaging"
    busName="Bus1"/>
</jmsQueueConnectionFactory>
```

```
<jmsQueue jndiName="jndi_INPUT_Q">
  <properties.wasJms queueName="QUEUE1" />
</jmsQueue>
```

– For Publish-Subscribe domain:

```
<jmsTopicConnectionFactory jndiName="eis/tcf">
  <properties.wasJms
    clientID="defaultID"
    remoteServerAddress="localhost:7276:BootstrapBasicMessaging"
    busName="Bus1"/>
</jmsTopicConnectionFactory>
```

```
<jmsTopic jndiName="eis/topic1">
  <properties.wasJms topicName="Football" />
</jmsTopic>
```

– For message-driven beans

Configure the activation specification property to all message-driven beans deployed in the Liberty server to connect to the messaging engine that is running on WebSphere Application Server traditional.

```
<jmsActivationSpec id="PriceChangeAS">
  <properties.wasJms
    destinationRef="jms/TriggerQ"
    remoteServerAddress="meserver.in.ibm.com:7276:BootstrapBasicMessaging busName="Bus1"/>
</jmsActivationSpec>

<jmsQueue id="jms/TriggerQ" jndiName="jms/TriggerQ">
  <properties.wasJms queueName="Q1"/>
</jmsQueue>
```

**Note:** If an application that is running on the Liberty server needs to connect to a messaging engine that is running on WebSphere Application Server traditional, then ensure that `remoteServerAddress` is configured to point to the server where the messaging engine is locally running instead of pointing to a Bootstrap server.

## Deploying JMS applications on the Liberty application client container



8.5.5.6

You can configure messaging applications that use `wasJmsClient-2.0` feature to run on the Liberty application client container.

### Before you begin

Before you can run an application client, you must create a client and add a configuration for your client application in the `client.xml` file. See the [Creating a Liberty application client manually](#) topic for examples of how you would create the application client.

### Procedure

1. To run the messaging application on the client, add the `javaeeClient-7.0` feature to the `client.xml` file.

```
<featureManager>
  <feature>javaeeClient-7.0</feature>
</featureManager>
```

2. Add the connection factory definitions to the `client.xml` file.

- For Point-to-Point domain:

```
<jmsQueueConnectionFactory jndiName="jndi_JMS_BASE_QCF" connectionManagerRef="ConMgr6">
  <properties.wasJms remoteServerAddress="localhost:7276:BootstrapBasicMessaging" />
</jmsQueueConnectionFactory>
<connectionManager id="ConMgr6" maxPoolSize="10"/>
```

```
<jmsQueue jndiName="jndi_INPUT_Q">
  <properties.wasJms queueName="QUEUE1" />
</jmsQueue>
```

- For Publish-Subscribe domain:

```
<jmsTopicConnectionFactory jndiName="eis/tcf">
  <properties.wasJms
    clientID="defaultID" />
</jmsTopicConnectionFactory>

<jmsTopic jndiName="eis/topic1">
  <properties.wasJms topicName="Football" />
</jmsTopic>
```

The JMS application is ready to run on the Liberty application client container.

# Enabling JMS tracing for the Liberty embedded messaging



8.5.5.6

JMS traces can be used in Liberty for problem determination and troubleshooting.

## Setting JMS traces

The following trace strings can be set in the `server.xml` file to obtain the required information.

### Connection problems

Use the following trace string to gather information about connection issues.

```
SIBTrm=all
```

### Communications and TCP/IP

Use the following trace string to gather information about the application server channel framework and TCP/IP network communications.

```
SIBCommunications=all:SIBJFapChannel=all:TCPChannel=fine:com.ibm.io.async.*=all
```

### JMS client applications

Use the following trace string to gather information about requests from JMS applications.

```
SIBJms*=all:SIBCommunications=all:SIBJFapChannel=all:  
SIBMessageTrace=all:SIBTrm=all:SIBJmsRa=all:SIBRa=all
```

### Locked messages

Use the following trace string if messages that are being delivered to MDBs and applications are locked for longer than you expect.

```
SIBProcessor=all:SIBMessageTrace=all
```

### Message-driven beans

Use the following trace string to gather information about MDBs that are configured by using an Activation Specification against a message destination.

```
SIBMessageTrace=all:SIBJmsRa=all:SIBRa=all
```

### Message format and schema

Use the following trace string if there is a problem in parsing or handling message data.

```
SIBMfp=all:SIBCommunications=all
```

### Message processor

Use the following trace string to gather information about the core functions of the messaging engine. Gathering this data is helpful, but might be potentially large.

```
SIBProcessor=all:SIBMessageTrace=all
```

### Message store

Use the following trace string to gather information about persistent message data, which is written out to storage so that it can be recovered if there is a failure.

```
SIBMessageStore=all
```

### Performance and message tracking

Use the following trace string to determine the delay in passing of messages or if you need to find where the messages are going.

```
SIBMessageTrace=all
```

### Publish/subscribe

Use the following trace string if subscribers are not getting the proper publications for their topic.

```
SIBMatchSpace=all:SIBProcessor=all
```

### Security

Use the following trace string if a user is authenticated incorrectly or is incorrectly allowed or disallowed access to resources.

```
SIBSecurity=all
```

## Deploying message-driven beans within Liberty

8.5.5.0

Liberty supports the configuration and deployment of message-driven beans (MDB) to process the JMS messages asynchronously from various destinations.

### Deploying message-driven beans to connect to WebSphere MQ



8.5.5.6

You can connect to WebSphere MQ by using the message-driven beans (MDB).

#### Procedure

1. Configure the MDB feature:

Enable MDB support in the Liberty server by configuring the `jmsMdb-3.2` and `wmqJmsClient-2.0` features in the `server.xml` file. If you want to perform a JNDI lookup, then you must also add the `jndi-1.0` feature along with the other two features.

```
<featureManager>
  <feature>jmsMdb-3.2</feature>
  <feature>wmqJmsClient-2.0</feature>
  <feature>jndi-1.0</feature>
</featureManager>
```

Configuring the `wmqJmsClient-2.0` feature enables the users to define the required JMS resources and enables MDB to interact with the messaging engine.

**Note:** The `wmqJmsClient-2.0` feature supports the features of both JMS 1.1 and JMS 2.0 specifications. However, you can choose to use the `wmqJmsClient-1.1` feature if you want to use only the features that are compliant with JMS 1.1 specification.

2. Specify the location of the WebSphere MQ Resource Adapter by adding the following entry to the `server.xml` file:

```
<variable name="wmqJmsClient.rar.location" value="/path/to/wmq/rar/wmq.jmsra.rar"/>
```

where the `value` attribute specifies the absolute path to the WebSphere MQ Resource Adapter file, `wmq.jmsra.rar`.

For details of the supported versions and obtaining the `wmq.jmsra.rar` file, refer to the WebSphere MQ technote 1633761. Obtain the `wmq.jmsra.rar` file and install it from Fix central.

3. Configure a JCA activation specification that uses the JMS resource adapter so that the MDB acts as a listener on a specific JMS destination. The following are different ways in which an MDB can be configured to interact with the messaging engine.

- a. Configure MDB by using the activation specification property.

You can define the property in the `server.xml` file so that the MDB can use the property to listen on a specific JMS destination.

```
<jmsActivationSpec id="JMSSample/JMSSampleMDB">
  <properties.wmqJms destinationRef="jndi/MDBQ" transportType="CLIENT" queueManager="myQM" hostName="myHost" port="1414"/>
</jmsActivationSpec>

<jmsQueue id="jndi/MDBQ" jndiName="jndi/MDBQ">
  <properties.wmqJms baseQueueName="MYQ" baseQueueManagerName="myQM"/>
</jmsQueue>
```

The `<destinationRef>` refers to the ID of `<jmsQueue>`. If an ID in `<jmsQueue>` is not mentioned, then `<destinationRef>` must point to the `<jndiName>` of the `<jmsQueue>`.

**Note:** The ID value must be in the format of application name/module name/bean name where

- *application name* is the name of the application that is deployed (for example, JMSSample). The application name applies only if the bean is packaged within an EAR file. The application defaults to the base name of the EAR file with no file name extension unless specified by the application.xml deployment descriptor.
  - *module name* is the name of the module in which the bean is packaged. In a stand-alone ejb-jar file or WAR file, the <module-name> defaults to the base name of the module with any file name extension removed. In an EAR file, the <module-name> defaults to the path name of the module with any file name extension removed, but with any directory names included. The default <module-name> can be overridden by using the module-name element of ejb-jar.xml (for ejb-jar files) or web.xml (for WAR files).
  - *bean name* is the ejb-name of the enterprise bean. For enterprise beans defined through annotation, the bean name defaults to the unqualified name of the session bean class, unless specified in the contents of the name() attribute of the MessageDriven annotation. For enterprise beans defined through ejb-jar.xml, it is specified in the <ejb-name> deployment descriptor element.
- b. Using annotations along with the activation specification property defined in the server.xml file. Liberty supports defining annotations for MDBs that can be used with the activation specification property defined in the server.xml file. In order to use the annotation, first define the activation specification property as mentioned in the previous step. And for each of the MDB, user can define the annotations as shown in the following example:

```
@MessageDriven(
    name = "JMSSampleMDB",
    activationConfig = {
        @ActivationConfigProperty(propertyName = "destinationType",
            propertyValue = "javax.jms.Queue"),
        @ActivationConfigProperty(propertyName = "userName",
            propertyValue = "user1"),
        @ActivationConfigProperty(propertyName = "password",
            propertyValue = "user1pwd"),
        @ActivationConfigProperty(propertyName = "destination",
            propertyValue = "jndi_INPUT_Q")
    }
)
public class JMSSampleMDB implements MessageListener{

    @TransactionAttribute(value = TransactionAttributeType.REQUIRED)
    public void onMessage(Message message) {
    }
}
```

- c. Using the EJB binding file (ibm-ejb-jar-bnd.xml).

You can also use this binding file to define the resource information that is required for the MDB to connect to the messaging engine. When you are using the EJB binding file, the activation specification property ID need not necessarily be in the format of application name/module name/bean name as mentioned in step 1.

Add the activation specification property information in the server.xml.

```
<jmsActivationSpec id="PriceChangeAS">
    <properties.wmqJms destinationRef="jms/TriggerQ" transportType="CLIENT" queueManager="myQM" hostName="myHost" port="1414"/>
</jmsActivationSpec>

<jmsQueue id="jms/TriggerQ" jndiName="jms/TriggerQ">
    <properties.wmqJms baseQueueName="Q1"/>
</jmsQueue>
```

Add the following MDB binding information in the ibm-ejb-jar-bnd.xml file.

```
<ejb-jar-bnd
xmlns="http://websphere.ibm.com/xml/ns/javaee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ejb-jar-bnd_1_1.xsd"
(http://websphere.ibm.com/xml/ns/javaee/ibm-ejb-jar-bnd_1_1.xsd%27) version="1.1">
```

```

<message-driven name="PriceChangeMDBBean">
  <jca-adapter activation-spec-binding-name="PriceChangeAS" destination-binding-name="jms/TriggerQ" />
</message-driven>
</ejb-jar-bnd>

```

**Note:** When using the EJB binding file, the **activation-spec-binding-name** attribute in the `ibm-ejb-jar-bnd.xml` file must point to the activation specification property ID value that is specified in the `server.xml` file.

## Deploying message-driven beans to connect to a JCA resource adapter

### 8.5.5.2

You can connect to a JCA resource adapter by using the message-driven beans (MDB).

### About this task

When you deploy a message-driven bean (MDB) application to Liberty, some configuration is required in the `server.xml` file to enable each MDB to receive messages from a resource adapter. The example configuration described in this topic is for an application that contains only message-driven beans and a JMS resource adapter. If the application will also use session beans, the `ejbLite-3.1` feature must be included.

Configuration properties will vary based on the specific resource adapter that is being used.

### Procedure

1. Configure the MDB feature:

Enable MDB support in Liberty by configuring the `mdb-3.1` and `jca-1.6` features in the `server.xml` file. If you want to perform a JNDI lookup, then you must also add the `jndi-1.0` feature along with the other two features.

```

<featureManager>
  <feature>mdb-3.1</feature>
  <feature>jca-1.6</feature>
  <feature>jndi-1.0</feature>
</featureManager>

```

2. Configure any other features required by your JCA resource adapter.
3. Configure a JCA activation specification that uses the resource adapter so that the MDB acts as a listener. The following examples show different ways that you can configure a MDB to interact with the messaging engine. These examples are specific to JMS resource adapters.
  - a. Configure MDB by using the activation specification property.

You can define the property in the `server.xml` file so that the MDB can use the property to listen on a specific JMS destination.

```

<activationSpec id="JMSSample/JMSSampleMDB">
  <properties.wmqJms destinationRef="jndi/MDBQ" transportType="CLIENT" queueManager="myQM" hostName="myHost" port="1414"/>
</activationSpec>

<jmsQueue id="jndi/MDBQ" jndiName="jndi/MDBQ">
  <properties.wmqJms baseQueueName="MYQ" baseQueueManagerName="myQM"/>
</jmsQueue>

```

The `<destinationRef>` refers to the ID of the `<jmsQueue>`. If an ID in the `<jmsQueue>` is not mentioned, then `<destinationRef>` element must point to the `<jndiName>` of the `<jmsQueue>`.

**Note:** The ID value must be in the format of application name/module name/bean name where

- *application name* is the name of the application that is deployed (for example, `JMSSample`). The application name applies only if the bean is packaged within an EAR file. The application defaults to the base name of the EAR file with no file name extension unless specified by the `application.xml` deployment descriptor.

- *module name* is the name of the module in which the bean is packaged. In a stand-alone ejb-jar file or WAR file, the <module-name> defaults to the base name of the module with any file name extension removed. In an EAR file, the <module-name> defaults to the path name of the module with any file name extension removed, but with any directory names included. The default <module-name> can be overridden by using the module-name element of ejb-jar.xml (for ejb-jar files) or web.xml (for WAR files).
  - *bean name* is the ejb-name of the enterprise bean. For enterprise beans defined through annotation, the bean name defaults to the unqualified name of the session bean class, unless specified in the contents of the name() attribute of the MessageDriven annotation. For enterprise beans defined through ejb-jar.xml, it is specified in the <ejb-name> deployment descriptor element.
- b. Configure the MDB by using annotations along with the activation specification property as defined in the server.xml file.

Liberty profile supports defining annotations for message-driven beans that can be used with the activation specification property defined in the server.xml file. To use the annotation, first define the activation specification property as mentioned in the previous step. And for each of the message-driven beans, you can define the annotations as shown in the following example:

```
@MessageDriven(
    name = "JMSSampleMDB",
    activationConfig = {
        @ActivationConfigProperty(propertyName = "destinationType",
            propertyValue = "javax.jms.Queue"),
        @ActivationConfigProperty(propertyName = "userName",
            propertyValue = "user1"),
        @ActivationConfigProperty(propertyName = "password",
            propertyValue = "user1pwd"),
        @ActivationConfigProperty(propertyName = "destination",
            propertyValue = "jndi_INPUT_Q")
    }
)
public class JMSSampleMDB implements MessageListener{

    @TransactionAttribute(value = TransactionAttributeType.REQUIRED)
    public void onMessage(Message message) {
    }
}
```

- c. Configure the MDB by using the EJB binding file ibm-ejb-jar-bnd.xml.

You can also use this binding file to define the resource information that is required for the MDB to connect to the messaging engine. When you are using the EJB binding file, the activation specification property ID is not required to be in the format of application name/module name/bean name as mentioned in step a.

Add the activation specification property information in the server.xml file.

```
<activationSpec id="PriceChangeAS">
    <properties.wmqJms destinationRef="jms/TriggerQ" transportType="CLIENT" queueManager="myQM" hostName="myHost" port="1414"/>
</activationSpec>

<jmsQueue id="jms/TriggerQ" jndiName="jms/TriggerQ">
    <properties.wmqJms baseQueueName="Q1"/>
</jmsQueue>
```

Add the following MDB binding information in the ibm-ejb-jar-bnd.xml file.

```
<ejb-jar-bnd
    xmlns="http://websphere.ibm.com/xml/ns/javaee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ejb-jar-bnd_1_1.xsd"
    (http://websphere.ibm.com/xml/ns/javaee/ibm-ejb-jar-bnd_1_1.xsd%27) version="1.1">

    <message-driven name="PriceChangeMDBBean">
        <jca-adapter activation-spec-binding-name="PriceChangeAS" destination-binding-name="jms/TriggerQ" />
    </message-driven>
</ejb-jar-bnd>
```

**Note:** When using the EJB binding file, the **activation-spec-binding-name** attribute in the `ibm-ejb-jar-bnd.xml` file must point to the activation specification property ID value that is specified in the `server.xml` file.

## Deploying message-driven beans to connect to the embedded messaging server



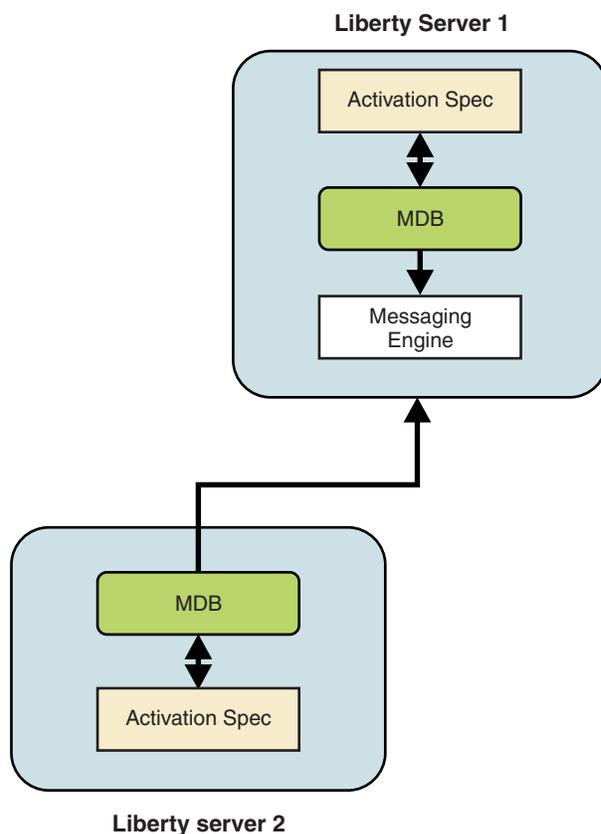
8.5.5.6

Use the message-driven beans (MDB) to connect to the embedded messaging server.

### About this task

MDB can be configured in the Liberty server in the following two scenarios:

- When both MDB and the messaging engine are on the same Liberty server.
- When MDB is connecting to a remote messaging engine that is running on a different Liberty server.



### Procedure

1. Configure the MDB feature:

Enable MDB support in the Liberty server by configuring the `javax.jms.Mdb-3.1` and `wasJmsClient-2.0` features in the `server.xml` file. If you want to perform a JNDI lookup, then you must also add the `javax.naming-1.0` feature along with the other two features.

```
<featureManager>
  <feature>javax.jms.Mdb-3.1</feature>
  <feature>wasJmsClient-2.0</feature>
  <feature>javax.naming-1.0</feature>
</featureManager>
```

Configuring the `wasJmsClient-2.0` feature enables the users to define the required JMS resources and enables MDB to interact with the messaging engine.

**Important:** The `wasJmsClient-2.0` feature supports the features of both JMS 1.1 and JMS 2.0 specifications. However, you can choose to use the `wasJmsClient-1.1` feature if you want to use only the features that are compliant with JMS 1.1 specification.

2. Configure a JCA activation specification that uses the JMS resource adapter so that the MDB acts as a listener on a specific JMS destination. The following are different ways in which an MDB can be configured to interact with the messaging engine.
  - a. Configure MDB by using the activation specification property.

You can define the property in the `server.xml` file so that the MDB can use the property to listen on a specific JMS destination.

```
<jmsActivationSpec id="JMSSample/JMSSampleMDB">
  <properties.wasJms destinationRef="jndi/MDBQ" />
</jmsActivationSpec>

<jmsQueue id="jndi/MDBQ" jndiName="jndi/MDBQ">
  <properties.wasJms queueName="Q1"/>
</jmsQueue>
```

The `<destinationRef>` refers to the ID of `<jmsQueue>`. If an ID in `<jmsQueue>` is not mentioned, then `<destinationRef>` must point to the `<jndiName>` of the `<jmsQueue>`.

**Note:** The ID value must be in the format of application name/module name/bean name where

- *application name* is the name of the application that is deployed (for example, `JMSSample`). The application name applies only if the bean is packaged within an EAR file. The application defaults to the base name of the EAR file with no file name extension unless specified by the `application.xml` deployment descriptor.
  - *module name* is the name of the module in which the bean is packaged. In a stand-alone `ejb-jar` file or `WAR` file, the `<module-name>` defaults to the base name of the module with any file name extension removed. In an EAR file, the `<module-name>` defaults to the path name of the module with any file name extension removed, but with any directory names included. The default `<module-name>` can be overridden by using the `module-name` element of `ejb-jar.xml` (for `ejb-jar` files) or `web.xml` (for `WAR` files).
  - *bean name* is the `ejb-name` of the enterprise bean. For enterprise beans defined through annotation, the bean name defaults to the unqualified name of the session bean class, unless specified in the contents of the `name()` attribute of the `MessageDriven` annotation. For enterprise beans defined through `ejb-jar.xml`, it is specified in the `<ejb-name>` deployment descriptor element.
- b. Using annotations along with the activation specification property defined in the `server.xml` file.

Liberty supports defining annotations for MDBs that can be used with the activation specification property defined in the `server.xml` file. In order to use the annotation, first define the activation specification property as mentioned in the previous step. And for each of the MDB, user can define the annotations as shown in the following example:

```
@MessageDriven(
  name = "JMSSampleMDB",
  activationConfig = {
    @ActivationConfigProperty(propertyName = "destinationType",
      propertyValue = "javax.jms.Queue"),
    @ActivationConfigProperty(propertyName = "userName",
      propertyValue = "user1"),
    @ActivationConfigProperty(propertyName = "password",
      propertyValue = "user1pwd"),
    @ActivationConfigProperty(propertyName = "destination",
      propertyValue = "jndi_INPUT_Q")
  }
)
public class JMSSampleMDB implements MessageListener{
```

```

    @TransactionAttribute(value = TransactionAttributeType.REQUIRED)
    public void onMessage(Message message) {
    }
}

```

c. Using the EJB binding file (ibm-ejb-jar-bnd.xml).

You can also use this binding file to define the resource information that is required for the MDB to connect to the messaging engine. When you are using the EJB binding file, the activation specification property ID need not necessarily be in the format of application name/module name/bean name as mentioned in step 1.

Add the activation specification property information in the server.xml.

```

<jmsActivationSpec id="PriceChangeAS">
  <properties.wasJms destinationRef="jms/TriggerQ" />
</jmsActivationSpec>

```

```

<jmsQueue id="jms/TriggerQ" jndiName="jms/TriggerQ">
  <properties.wasJms queueName="Q1"/>
</jmsQueue>

```

Add the following MDB binding information in the ibm-ejb-jar-bnd.xml file.

```

<ejb-jar-bnd
  xmlns="http://websphere.ibm.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://websphere.ibm.com/xml/ns/javaee http://websphere.ibm.com/xml/ns/javaee/ibm-ejb-jar-bnd_1_1.xsd
  (http://websphere.ibm.com/xml/ns/javaee/ibm-ejb-jar-bnd_1_1.xsd%27) version="1.1">
  <message-driven name="PriceChangeMDBBean">
    <jca-adapter activation-spec-binding-name="PriceChangeAS" destination-binding-name="jms/TriggerQ" />
  </message-driven>
</ejb-jar-bnd>

```

**Note:** When using the EJB binding file, the **activation-spec-binding-name** attribute in the ibm-ejb-jar-bnd.xml file must point to the activation specification property ID value that is specified in the server.xml file.

## Configuring connection pooling for JMS connections

### 8.5.5.1

You can customize the number of concurrent connections (default is 50) that can be created from a JMS connection factory. You can configure connection pooling for a specific JMS connection factory by defining the <connectionManager> element and then associate that element with the JMS connection factory in the server.xml file.

### Example

The connectionManager element in the server.xml file is used to the connection pool for a JMS connection factory property as given in the following example. The connection pool size is also defined in the connectionManager element.

```

<jmsConnectionFactory id="jmscf1"
  jndiName="jndi/example"
  connectionManagerRef="cm1">
  <properties.wasJms />
</jmsConnectionFactory>
<connectionManager id="cm1" maxPoolSize="10" minPoolSize="2" />

```

The server uses default values for any connection management settings that are not defined on the connectionManager element. If a connection manager is not defined for a connection factory, the server uses the default values for all the settings.

You can define multiple connection factories and associate each with a different connection manager. However, you cannot associate multiple connection factories with a single connection manager.

For more information about the `connectionManager` element, see .

---

## Deploying Java batch applications for Liberty



8.5.5.6

You can develop Java batch applications that are based on Java Specification Request (JSR) 352, and then submit Java batch jobs to run on a Liberty server.

### Java batch and managed batch overview



8.5.5.6

The Java batch function extends the application server to accommodate applications that must perform batch work alongside transactional applications. Batch work might take hours or even days to finish and uses large amounts of memory or processing power while it runs.

The Java Platform, Enterprise Edition Version 7 (Java EE 7) applications that are typically hosted by the product perform short, lightweight, transactional units of work. In most cases, an individual request can be completed with seconds of processor time and relatively little memory. Many applications, however, must complete batch work that is computational and resource-intensive.

Liberty supports the following batch features:

- Java batch

The `batch-1.0` feature enables the use of the JSR-352 programming model.

- Managed batch

The `batchManagement-1.0` feature provides the following functions:

- A REST interface for remote job submission
- The `batchManager` command-line utility
- Job logging support
- Multiple server support by using JMS

The `batch-1.0` and the `batchManagement-1.0` features support Java SE 7 and later.

**Note:** The `batchManagement-1.0` feature also enables the `batch-1.0` feature.

### Configuring Liberty for the batch REST API



8.5.5.6

WebSphere Application Server Liberty includes a RESTful management interface to manage your Java batch jobs. Managed batch enables a secure HTTPS REST interface so that you can externally manage your Java batch jobs.

#### Procedure

1. Add the `batchManagement-1.0` feature to your `server.xml` file.

```
<featureManager>
  <feature>batchManagement-1.0</feature>
</featureManager>
```

2. Configure batch persistence by configuring the **databaseStore** used by the Java batch feature. Reference the **databaseStore** in the `server.xml` file by using the **jobStoreRef** element. The following example illustrates what your `server.xml` file should look like.

```
<batchPersistence jobStoreRef="BatchDatabaseStore" />

<databaseStore id="BatchDatabaseStore" dataSourceRef="batchDB" />
```

For more information on database persistence, including auto-creation versus manual creation of tables, see Java batch persistence configuration.

3. Create an SSL certificate and user registry in your `server.xml` file, so that `batchManagement-1.0` automatically enables the SSL feature.

```
<keyStore id="defaultKeyStore" password="Liberty"/>

<basicRegistry id="basic" realm="ibm/api">
  <user name="bob" password="bobpwd" />
  <user name="jane" password="janepwd" />
</basicRegistry>
```

**Important:** The default self-signed SSL certificate in this example is intended only for development use and not for production.

For information on configuring role-based management of the batch environment and assigning users to roles, see [Securing the Liberty batch environment](#).

## Results

The RESTful interface is now configured for the Liberty server.

## Java batch persistence configuration



8.5.5.6

Java batch uses a persistent store to persist status, checkpoints, and application persistent data across multiple runs of a job instance. The persistent store enables a job instance to be restarted if an earlier run fails or must be stopped by supplying the restarted job with the appropriate data.

### Java batch memory-based persistence configuration

The batch persistence allows a job instance to be restarted if the execution ends in a `FAILED` or `STOPPED` state. In the absence of batch persistence configuration, Java batch uses a default capability of memory-based persistence to track status, checkpoints, and application persistent data across multiple runs of a job instance.

The default memory-based persistence implementation for Java batch is used by the underlying batch container when there is no `batchPersistence` and `databaseStore` elements present in the `server.xml` file.

**Note:** As a limitation for Java batch memory-based persistence, by default, persistence in Java batch is based on memory. If the batch container runtime or server JVM crash or are restarted, persistence is lost. This function is intended for development purposes only and is not to be considered for production systems or critical batch processing support.

### Java batch database persistence configuration

By default, the batch run time auto-creates non-existent tables based on the server configuration defined in the `databaseStore` element. The table definitions are customized based on the `schema` and `tablePrefix` attributes of the database store.

Alternatively, the `ddlGen` script can be used to generate a DDL based on the server configuration. If necessary, the DDL can be customized before manually creating the tables. This DDL also incorporates server configuration such as `schema` and `tablePrefix` and contains the appropriate SQL for the database type of the data source referenced by the `databaseStore`.

**Note:** Customized DDL must use positive integer primary key IDs. As a limitation for database persistence, Java Batch does not accept negative or zero integer IDs persisted in the primary key identity columns. The Java Batch container runtime only runs jobs that use positive integer job IDs persisted in the primary key identity columns.

The auto-creation of tables can be disabled by using the `createTables="false"` attribute on the `databaseStore`. This option can be used to ensure that you use manually created tables instead of using auto-created tables if the batch runtime unexpectedly could not find your manually created tables.

The samples shown on this page use the default auto-create behavior. This behavior is equivalent to `createTables="true"`.

**Note:** To avoid data integrity issues that are caused by having an isolation level less than `REPEATABLE_READ`, set the isolation level of the data source to `TRANSACTION_REPEATABLE_READ`. If you do not specify an isolation level, the default depends on the database. In most cases, the default is `TRANSACTION_REPEATABLE_READ`.

## Persistence configuration sample

The following sample configures batch access to the automatically created target database table `RUNTIMEDB` for Derby.

```
<!-- Batch persistence config. References a databaseStore. -->
<batchPersistence jobStoreRef="BatchDatabaseStore" />

<!-- The database store for the batch tables. -->
<!-- Note this database store is referenced by the batchPersistence element. -->
<databaseStore id="BatchDatabaseStore" dataSourceRef="batchDB" schema="JBATCH" tablePrefix="" />

<!-- Derby JDBC driver -->
<!-- Note this library is referenced by the dataSource element -->
<library id="DerbyLib">
  <fileset dir="{server.config.dir}/resources/derby" />
</library>

<!-- Data source for the batch tables. -->
<!-- Note this data source is referenced by databaseStore element -->
<dataSource id="batchDB" isolationLevel="TRANSACTION_REPEATABLE_READ" >
  <jdbcDriver libraryRef="DerbyLib" />
  <properties.derby.embedded
    databaseName="{server.config.dir}/resources/RUNTIMEDB"
    createDatabase="create"
    user="user"
    password="pass" />
</dataSource>
```

## Securing the Liberty batch environment



8.5.5.6

The Liberty batch framework allows you to configure role-based access to all batch management operations and also to view metadata and logs associated with your batch jobs.

### Before you begin

Three batch roles are defined by the batch container. A single user can have more than one batch role.

#### **batchAdmin**

A `batchAdmin` has unrestricted access to all batch operations. This includes permission to submit

new jobs, stop and restart any user's jobs, view any job metadata and job logs that are submitted by any user in the batch domain, and to purge any jobs. A batchAdmin is not necessarily a WebSphere Application Server administrator.

### batchSubmitter

A batchSubmitter has permission to submit new jobs and can only perform batch operations such as stop, restart, or purge on their own jobs. A batchSubmitter cannot view or modify other user's jobs. For example, if user1 and user2 are defined as batchSubmitters, and user1 submits a job, user2 cannot view the job instance data that is associated with user1's job.

### batchMonitor

A batchMonitor has read-only permissions to all jobs. Users in this role can view all job instances and executions and have access to all job logs. A batchMonitor cannot submit their own jobs, or stop, restart, or purge any jobs.

**Note:** Once batch security is enabled, any JobOperator API method or REST operation that returns a list will be filtered based on the batch roles granted to the current user. For example, when a user with only batchSubmitter permissions requests a list of all job instances, only job instances submitted by the current user will be returned.

## About this task

### Procedure

1. By default, the batch-1.0 feature does not enable any security. The JobOperator methods are left open for all users whether they are authenticated or not. The methods are left open for development purposes only and require no security configuration. The batchManagement-1.0 feature enables the batch REST API. The REST API always requires a user to authenticate even when the appSecurity-2.0 feature is not enabled, but all users will be treated as batch administrators and can perform all batch operations on any job instance. Once appSecurity-2.0 is enabled, batch role-based security authorization will be performed and users will be restricted to batch operations defined by their given batch roles.

- a. Enable the batch role-based security through the JobOperator API

```
<featureManager>
  <feature>batch-1.0</feature>
  <feature>appSecurity-2.0</feature>
</featureManager>
```

- b. Enable the batch role-based security through the REST API.

**Note:** The batchManagement-1.0 feature includes the batch-1.0 feature.

```
<featureManager>
  <feature>batchManagement-1.0</feature>
  <feature>appSecurity-2.0</feature>
</featureManager>
```

2. Configure your server.xml file to support role-based security. The following example illustrates a basic user registry that defines a list of users. This registry is used by sample batch role based security configurations.

```
<basicRegistry id="basic" realm="ibm/api">
  <user name="alice" password="alicepwd" />
  <user name="bob" password="bobpwd" />
  <user name="jane" password="janepwd" />
  <user name="joe" password="joepwd" />
  <user name="phyllis" password="phyllispwd" />
  <user name="kai" password="kaipwd" />
</basicRegistry>
```

In this example, one user occupies multiple roles.

```
<authorization-roles id="com.ibm.ws.batch">
  <security-role name="batchAdmin" >
    <user name="alice" />
```

```

</security-role>
<security-role name="batchSubmitter" >
  <user name="jane" />
  <user name="phyllis" />
  <user name="bob" />
</security-role>
<security-role name="batchMonitor" >
  <user name="joe" />
  <user name="bob" />
</security-role>
</authorization-roles>

```

In this example, one user occupies multiple roles. All users have the batchSubmitter role.

```

<authorization-roles id="com.ibm.ws.batch">
  <security-role name="batchAdmin" >
    <user name="alice" />
  </security-role>
  <security-role name="batchSubmitter" >
    <special-subject type="ALL_AUTHENTICATED_USERS"/>
  </security-role>
  <security-role name="batchMonitor" >
    <user name="joe" />
    <user name="bob" />
  </security-role>
</authorization-roles>

```

In this example, one user occupies multiple roles. All users, including those users that are not authenticated, are allowed to have the batchMonitor role.

```

<authorization-roles id="com.ibm.ws.batch">
  <security-role name="batchAdmin" >
    <user name="alice" />
  </security-role>
  <security-role name="batchSubmitter" >
    <user name="joe" />
    <user name="bob" />
  </security-role>
  <security-role name="batchMonitor" >
    <special-subject type="EVERYONE"/>
  </security-role>
</authorization-roles>

```

z/OS

**Note:** If the zosSecurity-1.0 feature is enabled, then batch role-based authorization is handled by the SAF authorization provider.

The SAF authorization provider determines the authorization of the client by checking the client's access level to SAF resource profiles defined in the EJBROLE class. By default, the following resource profiles are associated with the batch roles.

```

batchAdmin:    BBGZDFLT.com.ibm.ws.batch.batchAdmin
batchSubmitter: BBGZDFLT.com.ibm.ws.batch.batchSubmitter
batchMonitor:  BBGZDFLT.com.ibm.ws.batch.batchMonitor

```

The client identity must be granted READ access to the appropriate resource profile to be authorized to the corresponding batch role.

The following example illustrates the RACF commands to grant the client identity, bob, authorization to the batchAdmin role.

```

RDEFINE EJBROLE BBGZDFLT.com.ibm.ws.batch.batchAdmin UACC(NONE)
PERMIT BBGZDFLT.com.ibm.ws.batch.batchAdmin CLASS(EJBROLE) ID(bob) ACCESS(READ)

```

## Java batch shutdown and recovery



8.5.5.6

The Java batch feature behaves differently when the server is shut down while jobs are still running.

### Deactivating Java batch

Java batch is deactivated when the server is stopped or the Java batch feature is removed. It is also deactivated and reactivated to process a dynamic configuration update. Deactivating Java batch causes stop requests to be issued to all active jobs and messages to be logged for each stop. There is a 2-second period for the jobs to stop. If after 2 seconds there are Java batch jobs that are still running, a message is logged that indicates which job execution IDs are still active. Java batch then shuts down. If jobs are still running after Java batch shuts down, they can experience unpredictable behavior.

**Important:** If the server is unexpectedly stopped, Java batch recovers by marking all jobs that were running on the server but not completed as FAILED when the server is restarted.

### Batch REST API



8.5.5.6

The WebSphere Application Server Liberty includes a RESTful management interface to manage your batch jobs.

The basic operations that are associated with a batch job are to submit (start), stop, restart, and view status. You can perform these operations by using any HTTP REST client. Any data that is submitted as part of a request or returned as part of a response is JSON formatted.

The following examples show the functions that you can perform with the REST API.

**Note:** The Batch REST API is versioned on a URL by URL basis. URL's with no version number are considered as version 1 of the API. The web addresses of the batch REST interface all start with the root web address: `https://{host}:{port}/ibm/api/batch/{version}/`.

**Remember:** The web addresses of the batch REST interface all start with the root web address: `https://{host}:{port}/ibm/api/batch`.

- “REST API with a user ID that is only a submitter”
- “Job instances” on page 2214
- “Job executions” on page 2221
- “Step executions” on page 2222
- “Job logs” on page 2225
- “HTTP Return Codes” on page 2226
- “STOP requests in a distributed server batch environment” on page 2226
- “JOBLOGS requests in a distributed server batch environment” on page 2226
- “Purge requests in a distributed server batch environment” on page 2227

### REST API with a user ID that is only a submitter

The results returned by the GET (“read”) URLs will be filtered when the user ID that invokes the REST API over HTTPS has only been granted access to the **batchSubmitter** role. The submitter only sees instance and execution data that is associated with job instances that were submitted by the submitter himself. In contrast, user ids granted access to the **batchAdmin** and **batchMonitor** roles will be able to view all instance and execution data (returned by any given URL with any given set of parameters).

A userid which only has access to the **batchSubmitter** role sees results that are first filtered by the standard parameters as described in the documentation of the given URL, and then further filtered by only returning instance and execution data associated with job instances submitted by the submitter himself.

See *Securing the Liberty batch environment* for more information.

## Job instances

### GET /ibm/api/batch/jobinstances/

This URI returns a list of job instances. Query parameters include:

- `page=[page number]`: Indicates which page (subset of records) to return. The default is 0.
- `pageSize=[number of records per page]`: Indicates the number of records per page. The default is 50.

Sample requests:

```
https://localhost:9443/ibm/api/batch/jobinstances
```

```
https://localhost:9443/ibm/api/batch/jobinstances?page=13&pagesize=20
```

Sample response:

```
[
  {
    "jobName": "test_sleepyBatchlet",
    "instanceId": 7,
    "appName": "SimpleBatchJob#SimpleBatchJob.war",
    "submitter": "bob",
    "batchStatus": "COMPLETED",
    "jobXMLName": "test_sleepyBatchlet",
    "instanceState": "COMPLETED",
    "_links": [
      {
        "rel": "self",
        "href": "https://localhost:9443/ibm/api/batch/jobinstances/7"
      },
      {
        "rel": "job logs",
        "href": "https://localhost:9443/ibm/api/batch/jobinstances/7/joblogs"
      }
    ]
  },
  {
    "jobName": "test_sleepyBatchlet",
    "instanceId": 6,
    "appName": "SimpleBatchJob#SimpleBatchJob.war",
    "submitter": "bob",
    "batchStatus": "COMPLETED",
    "jobXMLName": "test_sleepyBatchlet",
    "instanceState": "COMPLETED",
    "_links": [
      {
        "rel": "self",
        "href": "https://localhost:9443/ibm/api/batch/jobinstances/6"
      },
      {
        "rel": "job logs",
        "href": "https://localhost:9443/ibm/api/batch/jobinstances/6/joblogs"
      }
    ]
  }
]
```

### GET /ibm/api/batch/v2/jobinstances/

This URI returns a list of job instances filtered by the following query parameters:

- `jobInstanceId=[instanceId]:[instanceId]`: Returns job instances equal to and between the `instanceId` range.
- `jobInstanceId=>[instanceId]`: Returns job instances equal to and greater than the provided `instanceId`.
- `jobInstanceId=<[instanceId]`: Returns job instances equal to and less than the provided `instanceId`.
- `jobinstanceId=[instanceId],[instanceId],[instanceId]`: Returns job instances specified.
- `createTime=[yyyy-MM-dd]:[yyy-MM-dd]`: Returns job instances between the date range inclusively. For more information, see note further on in this topic.
- `createTime=[yyyy-MM-dd]`: Returns job instances on the given date. For more information, see note further on in this topic.
- `createTime=>3d`: Returns job instances that were created on or after the day which was three days ago. For example, the `createTime` is greater than or equal to the beginning of the day three days ago. For more information, see note further on in this topic.
- `createTime=<3d`: Returns job instances that were created on or before the day which was three days ago. For example, the `createTime` is less than or equal to the end of the day three days ago. For more information, see note further on in this topic.
- `instanceState=[state],[state]`: Returns job instances with the provided state. Valid Instance States are SUBMITTED, JMS\_QUEUED, JMS\_CONSUMED, DISPATCHED, FAILED, STOPPED, COMPLETED and ABANDONED.
- `exitStatus=[string]`: Returns job instances matching the exit status string. The string criteria may utilize the wildcard(\*) operator on either end.
- `page=[page number]`: Indicates which page (subset of records) to return. The default is 0.
- `pageSize=[number of records per page]`: Indicates the number of records per page. The default is 50.

**Note: The role of the server default timezone in queries involving createTime**

When you submit a job, the `createTime` for the job instance is stored in the job repository and normalized to UTC. When specifying dates via `yyyy-MM-dd`, as in `createTime=[yyyy-MM-dd]` or `createTime=[yyyy-MM-dd]:[yyy-MM-dd]:`, then you must convert the `yyyy-MM-dd` date string into a specific range of UTC times to match against the `createTime` values in the job instance table records. To do this, the application uses the default timezone of the server handling the REST request. It is this server's timezone that is used to convert the date string into a UTC time range that will be matched against.

The following table illustrates data returned by the query parameters **jobInstanceId=10:13**.

JOBINSTANCEID	CREATETIME(* in server1's timezone)	INSTANCESTATE	EXITSTATUS
10	11-05-2015.01:10:00	COMPLETED	SUCCESS
11	11-08-2014.02:20:00	COMPLETED	SUCCESS
12	11-10-2015.03:30:00	FAILED	FAILURE
13	11-11-2015.04:40:00	COMPLETED	SUCCESS

\*Since the job repository stores the `createTime` in a UTC format, it is important to understand that the table data above shows the `createTime` formatted using the server's default timezone of a particular server, for example, "server1". If we had constructed a similar table from the perspective of a second server with a different default timezone (than "server1"), we would show a different set of `CREATETIME` column values which a corresponding timezone-based difference. It is the default timezone of the server handling the REST request which is used to map `yyyy-MM-dd` date string parameters to UTC `createTime` values in the database in the examples below.

The following commands return the same result regardless of which server they are issued against:

- `jobInstanceId=11:13` would return JOBINSTANCEID's 11, 12 and 13.
- `jobInstanceId=>12` would return JOBINSTANCEID's 12 and 13.
- `jobInstanceId=<12` would return JOBINSTANCEID's 11 and 12.
- `jobInstanceId=11,12` would return JOBINSTANCEID's 11 and 12.
- `instanceState=FAILED` would return JOBINSTANCEID 12..
- `exitStatus=SUCCESS` would return JOBINSTANCEID's 10, 11 and 13.

The following commands may return different results against servers with different default timezones. In these examples, they are issued against "server1" (the same server used to populate the table above) at date and time: 11-11-2015:07:00:00 in the server's default timezone.

- `createTime=>2d` would return JOBINSTANCEID's 12 and 13 (on or after 2 days ago, which was 11-09-2015)
- `createTime=<2d` would return JOBINSTANCEID's 10 and 11 (on or before 2 days ago, which was 11-09-2015)
- `createTime=2015-11-08:2015-11-11` would return records with JOBINSTANCEID's 11,12, and 13.
- `createTime=2015-11-10` would return record with JOBINSTANCEID 12.

Sample requests:

```
https://localhost:9443/ibm/api/batch/v2/jobinstances?instanceId=20:50
```

```
https://localhost:9443/ibm/api/batch/jobinstances?createTime=>2d
```

```
https://localhost:9443/ibm/api/batch/v2/jobinstances?instanceId=4,12,17&instanceState=COMPLETED
```

```
https://localhost:9443/ibm/api/batch/v2/jobinstances?instanceId=4500:4600&createTime=2015-11-27&instanceState=COMPLETED
```

#### **GET /ibm/api/batch/jobinstances/job *instance id***

This URI returns detailed information about the specified job instance such as all executions that are associated with a specified job instance. Results are returned in order from most recent to the oldest. The most recent result is displayed first in the list.

Sample response:

```
{
  "jobName": "test_sleepyBatchlet",
  "instanceId": 7,
  "appName": "SimpleBatchJob#SimpleBatchJob.war",
  "submitter": "bob",
  "batchStatus": "COMPLETED",
  "jobXMLName": "test_sleepyBatchlet",
  "instanceState": "COMPLETED",
  "_links": [
    {
      "rel": "self",
      "href": "https://localhost:9443/ibm/api/batch/jobinstances/7"
    },
    {
      "rel": "job logs",
      "href": "https://localhost:9443/ibm/api/batch/jobinstances/7/joblogs"
    },
    {
      "rel": "job execution",
      "href": "https://localhost:9443/ibm/api/batch/jobinstances/7/jobexecutions/7"
    }
  ]
}
```

#### **POST /ibm/api/batch/jobinstances/**

Use this URI to submit (start) a new job.

The following example illustrates the request body for submitting a job that is packaged in a WAR module, in JSON formatting:

```
{
  "applicationName" : "SimpleBatchJob",
  "moduleName" : "SimpleBatchJob.war",
  "jobXMLName" : "test_batchlet_jsl",
  "jobParameters" : { "prop1" : "prop1value", "prop2" : "prop2value"}
}
```

The following example illustrates the request body for submitting a job that is packaged in an EJB module, in JSON formatting:

```
{
  "applicationName" : "SimpleBatchJob",
  "moduleName" : "SimpleBatchJobEJB.jar",
  "componentName" : "MyEJB",
  "jobXMLName" : "test_batchlet_jsl",
  "jobParameters" : { "prop1" : "prop1value", "prop2" : "prop2value"}
}
```

The *applicationName* identifies the batch application. It is required unless *moduleName* is specified, in which case the *applicationName* is derived from the *moduleName* by trimming off the .war or .jar suffix of the *moduleName*. For example, if you provide no *applicationName* and *moduleName*=SimpleBatchJob.war, then *applicationName* defaults to SimpleBatchJob.

The *moduleName* identifies the module within the batch application that contains the job artifacts, such as the JSL. The job is submitted under the module's component context. The *moduleName* is required unless *applicationName* is specified, in which case the *moduleName* is derived from the *applicationName* by appending .war to the *applicationName*. For example, if you provide *applicationName*=SimpleBatchJob and no *moduleName*, then *moduleName* defaults to SimpleBatchJob.war.

The *componentName* identifies the EJB component within the batch application EJB module. If specified, the job is submitted under the EJB's component context.

**Note:** The *componentName* is required only when the module is an EJB module. When the module is a WAR module, the *componentName* is not required.

You must enter a value for *jobXMLName*. The value for *jobParameters* is optional.

**8.5.5.7** As an alternative to using the JSL job definition that is packaged within your batch application under META-INF/batch-jobs, you can pass your JSL inline as part of your REST job submission request. The JSL that is submitted inline always overrides any JSL that is packaged with the batch application. There are two ways to submit your JSL inline as part of your HTTP request.

1. Include your JSL as a JSON property in your job submission request. Add the property **jobXML** to the JSON object and add the entire content of the JSL file as a JSON string as the value of the property.

**Note:** You must properly escape the XML string so it can be parsed by a JSON parser. Most JSON libraries will do this for you.

The following example illustrates the request body for submitting a job that utilizes a single part HTTP request with the JSL being passed in-line by the JSON.

```
{
  "applicationName":"SimpleBatchJob",
  "jobXMLName":"test_multiPartition_3Steps",
  "jobXML":"<?xml version='1.0' encoding='UTF-8'>
standalone='yes'?>
\r\n<job id='test_multiPartition_3Steps'
xmlns='http://xmlns.jcp.org/xml/ns/javaee'\r\n\tversion='1.0'>
\r\n\t<step id='step1' next='step2'>
\r\n\t\t<batchlet ref='simpleBatchlet' />
\r\n\t\t<partition>\r\n\t\t\t<plan partitions='3' />
\r\n\t\t</partition>\r\n\t\t</step>
\r\n\t<step id='step2' next='step3'>
```

```

\r\n\t\t<batchlet ref="simpleBatchlet" />
\r\n\t\t<partition>\r\n\t\t\t<plan partitions="3" />
\r\n\t\t</partition>\r\n\t\t</step>\r\n\t\t<step id="step3">
\r\n\t\t\t<batchlet ref="simpleBatchlet" />\r\n\t\t</partition>
\r\n\t\t\t<plan partitions="3"/>
\r\n\t\t</partition>\r\n\t\t</step>\r\n</job>"
}

```

**Note:** The **jobXML** field must be parsed by a JSON parser and marshalled into a valid JSON object. The **jobXMLName** field is optional, as the job ID information in the inline JSL is used for the job name.

2. Use an HTTP multi-part form. When you use an HTTP multipart form the JSON job submission data and XML job definition need to be submitted as two separate parts of the HTTP body. The JSON part of the multi-part form must be named *jobdata* and the XML part of the form must be named *jsl*. The XML does not need to be marshalled to a JSON string when you use a multi-part form.

The following example illustrates the HTTP request for submitting a job that uses a multi-part HTTP request with the JSL being passed inline via the *jsl* message part.

```
Content-Type: multipart/form-data;boundary=-----49424d5f4a4241544348
```

```
-----49424d5f4a4241544348
```

```
Content-Disposition: form-data; name="jobdata"
```

```
Content-Type: application/json; charset=UTF-8
```

```
{
  "applicationName" : "SimpleBatchJob",
  "moduleName" : "SimpleBatchJob.war",
  "jobXMLName" : "test_multiPartition"
}
```

```
-----49424d5f4a4241544348
```

```
Content-Disposition: form-data; name="jsl"
```

```
Content-Type: application/xml; charset=UTF-8
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<job id="test_multiPartition" xmlns="http://xmlns.jcp.org/xml/ns/javaee"
version="1.0">
<step id="step1">
<batchlet ref="simpleBatchlet" />
<partition>
  <plan partitions="3" />
</partition>
</step>
</job>
```

```
-----49424d5f4a4241544348--
```

**Note:** The **jobXMLName** field is optional, as the job ID information in the inline JSL is used for the job name.

The following sample response illustrates a successful job submission:

```
{
  "jobName": "test_sleepyBatchlet",
  "instanceId": 10,
  "appName": "SimpleBatchJob#SimpleBatchJob.war",
  "submitter": "bob",
  "batchStatus": "STARTING",
  "jobXMLName": "test_sleepyBatchlet",
  "instanceState": "SUBMITTED",
  "_links": [
    {
      "rel": "self",
      "href": "https://localhost:9443/ibm/api/batch/jobinstances/10"
    }
  ],
}
```

```

    {
      "rel": "job logs",
      "href": "https://localhost:9443/ibm/api/batch/jobinstances/10/joblogs"
    }
  ]
}

```

**PUT /ibm/api/batch/jobinstances/job *instance id*?action=stop**

Use this URI to stop the most recent job execution that is associated with this job instance if it is running. If it is not, the API returns an error.

**PUT /ibm/api/batch/jobinstances/job *instance id*?action=restart**

Use this URI to restart the most recent job execution that is associated with this job instance only if it is in STOPPED or FAILED state. If no job execution is associated with this instance, or the latest job execution is in COMPLETED state, the API returns an error.

**PUT /ibm/api/batch/jobinstances/job *instance id*?action=restart&reusePreviousParams=true**

Use this URI to restart the most recent job execution and reuse the job parameters from the previous execution that is associated with this job instance. The previous execution must be in STOPPED or FAILED state. If no job execution is associated with this instance, or the latest job execution is in COMPLETED state, then the API returns an error. Note that **reusePreviousParams** is an optional setting. The default setting is **reusePreviousParams=false**.

**Note:** When **reusePreviousParams=true**, any job parameters that are submitted as part of the current restart request take precedence over any previous job parameters. Current parameters override previous parameters with the same job parameter key name.

**DELETE /ibm/api/batch/jobinstances/job *instance id***

This URI purges all database entries and job logs that are associated with this job instance. This API returns an error if the job instance has active job executions. If there is an error when you delete the job logs, then no attempt is made to delete the job instance data from the job store database. Query parameters include:

- `purgeJobStoreOnly=true|false`: When `purgeJobStoreOnly=true`, no attempt is made to purge the job logs associated with this job instance. The default setting is `purgeJobStoreOnly=false`. This API returns an error if the job instance has active job executions.

**Note:** No purge response message is returned when you utilize the single purge API.

**DELETE /ibm/api/batch/v2/jobinstances/**

This URI purges all database entries and job logs associated with the job instances returned by the following purge filter parameters:

**Note:** It is recommended that you utilize the GET interface to list out the jobs and verify they are the correct jobs to purge before performing the DELETE interface to purge them.

- `page=[page number]`: Indicates which page (subset of records) to return. The default is 0
- `pageSize=[number of records per page]`: Indicates the number of records per page. The default is 50.
- `purgeJobStoreOnly=true|false`: When `purgeJobStoreOnly=true`, no attempt is made to purge the job logs associated with this job instance. The default setting is `purgeJobStoreOnly=false`. This API returns an error if the job instance has active job executions.
- `jobInstanceId=[instanceId]:[instanceId]`: Purges job instances equal to and between the `instanceId` range.
- `jobInstanceId=>[instanceId]`: Purges job instances equal to and greater than the provided `instanceId`.
- `jobInstanceId=<[instanceId]`: Purges job instances equal to and less than the provided `instanceId`.
- `jobinstanceId=[instanceId],[instanceId],[instanceId]`: Purges job instances specified.

- createTime=[yyyy-MM-dd]:[yyy-MM-dd]: Returns job instances between the date range inclusively. For more information, see note further on in this topic.
- createTime=[yyyy-MM-dd]: Returns job instances on the given date. For more information, see note further on in this topic.
- createTime=>3d: Returns job instances that were created on or after the day which was three days ago. For example, the createTime is greater than or equal to the beginning of the day three days ago. For more information, see note further on in this topic.
- createTime=<3d: Returns job instances that were created on or before the day which was three days ago. For example, the createTime is less than or equal to the end of the day three days ago. For more information, see note further on in this topic.
- instanceState=[state],[state]: Purges job instances with the provided state. Valid Instance States are SUBMITTED, JMS\_QUEUED, JMS\_CONSUMED, DISPATCHED, FAILED, STOPPED, COMPLETED, and ABANDONED.
- exitStatus=[string]: Returns job instances matching the exit status string. The string criteria may utilize the wildcard(\*) operator on either end.

**Note:** By default, unless the page and pageSize parameters are specified, a maximum of 50 records are purged.

**Note: The role of the server default timezone in queries involving createTime**

When you submit a job, the createTime for the job instance is stored in the job repository and normalized to UTC. When specifying dates via yyyy-MM-dd, as in createTime=[yyyy-MM-dd] or createTime=[yyyy-MM-dd]:[yyy-MM-dd]:, then you must convert the yyyy-MM-dd date string into a specific range of UTC times to match against the createTime values in the job instance table records. To do this, the application uses the default timezone of the server handling the REST request. It is this server's timezone that is used to convert the date string into a UTC time range that will be matched against.

The following table illustrates data returned by the query parameters **jobInstanceId=10:13**.

JOBINSTANCEID	CREATETIME(* in server1's timezone)	INSTANCESTATE	EXITSTATUS
10	11-05-2015.01:10:00	COMPLETED	SUCCESS
11	11-08-2014.02:20:00	COMPLETED	SUCCESS
12	11-10-2015.03:30:00	FAILED	FAILURE
13	11-11-2015.04:40:00	COMPLETED	SUCCESS

\*Since the job repository stores the createTime in a UTC format, it is important to understand that the table data above shows the createTime formatted using the server's default timezone of a particular server, for example, "server1". If we had constructed a similar table from the perspective of a second server with a different default timezone (than "server1"), we would show a different set of CREATETIME column values which a corresponding timezone-based difference. It is the default timezone of the server handling the REST request which is used to map yyyy-MM-dd date string parameters to UTC createTime values in the database in the examples below.

The following commands return the same result regardless of which server they are issued against:

- jobInstanceId=11:13 would return JOBINSTANCEID's 11, 12 and 13.
- jobInstanceId=>12 would return JOBINSTANCEID's 12 and 13.
- jobInstanceId=<12 would return JOBINSTANCEID's 11 and 12.
- jobInstanceId=11,12 would return JOBINSTANCEID's 11 and 12.
- instanceState=FAILED would return JOBINSTANCEID 12..

- `exitStatus=SUCCESS` would return `JOBINSTANCEID`'s 10, 11 and 13.

The following commands may return different results against servers with different default timezones. In these examples, they are issued against "server1" (the same server used to populate the table above) at date and time: 11-11-2015:07:00:00 in the server's default timezone.

- `createTime=>2d` would return `JOBINSTANCEID`'s 12 and 13 (on or after 2 days ago, which was 11-09-2015)
- `createTime=<2d` would return `JOBINSTANCEID`'s 10 and 11 (on or before 2 days ago, which was 11-09-2015)
- `createTime=2015-11-08:2015-11-11` would return records with `JOBINSTANCEID`'s 11,12, and 13.
- `createTime=2015-11-10` would return record with `JOBINSTANCEID` 12.

Sample response:

```
[{"instanceId":394,"purgeStatus":"COMPLETED","message":"Successful purge.,"redirectUrl":""},
{"instanceId":395,"purgeStatus":"COMPLETED","message":"Successful purge.,"redirectUrl":""},
{"instanceId":396,"purgeStatus":"COMPLETED","message":"Successful purge.,"redirectUrl":""},
{"instanceId":397,"purgeStatus":"COMPLETED","message":"Successful purge.,"redirectUrl":""},
{"instanceId":398,"purgeStatus":"COMPLETED","message":"Successful purge.,"redirectUrl":""}]
```

The following `purgeStatus` values can be returned:

#### **COMPLETED**

Indicates that the job purge completed successfully.

#### **FAILED**

Indicates that the job purge failed.

#### **STILL\_ACTIVE**

Indicates that the job purge failed because it was still active.

#### **JOBLOGS\_ONLY**

Indicates that the database purge failed, but that the job logs were successfully purged.

#### **NOT\_LOCAL**

Indicates that the job purge failed because the job is not local.

## **Job executions**

### **GET /ibm/api/batch/jobexecutions/*job execution id***

This URI returns detailed information about a specified job execution and includes links to associated step executions and job logs.

Sample request:

```
https://localhost:9443/ibm/api/batch/jobexecutions/9
```

Sample response:

```
{
  "jobName":"test_sleepyBatchlet",
  "executionId":9,
  "instanceId":9,
  "batchStatus":"COMPLETED",
  "exitStatus":"COMPLETED",
  "createTime":"2015/05/07 16:09:41.025 -0400",
  "endTime":"2015/05/07 16:09:52.127 -0400",
  "lastUpdatedTime":"2015/05/07 16:09:52.127 -0400",
  "startTime":"2015/05/07 16:09:41.327 -0400",
  "jobParameters":{
  },
  "restUrl":"https://localhost:9443/ibm/api/batch",
  "serverId":"localhost/C:/ibm/RAD_workspaces/Liberty7/build.image/wlp/usr/server1",
  "logpath":"C:\\ibm\\Liberty\\wlp\\usr\\servers\\server1\\logs\\joblogs\\test_sleepyBatchlet\\2015-05-07\\ins",
  "stepExecutions":[
  ]
}
```

```

        "stepExecutionId":9,
        "stepName":"step1",
        "batchStatus":"COMPLETED",
        "exitStatus":"SleepyBatchlet:i=10;stopRequested=false",
        "stepExecution":"https://localhost:9443/ibm/api/batch/jobexecutions/9/stepexecutions/step1"
    },
    "_links":[
        {
            "rel":"self",
            "href":"https://localhost:9443/ibm/api/batch/jobexecutions/9"
        },
        {
            "rel":"job instance",
            "href":"https://localhost:9443/ibm/api/batch/jobinstances/9"
        },
        {
            "rel":"step executions",
            "href":"https://localhost:9443/ibm/api/batch/jobexecutions/9/stepexecutions"
        },
        {
            "rel":"job logs",
            "href":"https://localhost:9443/ibm/api/batch/jobexecutions/9/joblogs"
        },
        {
            "rel":"stop url",
            "href":"https://localhost:9443/ibm/api/batch/jobexecutions/9?action=stop"
        }
    ]
}

```

#### **GET /ibm/api/batch/jobexecutions/job execution id/jobinstance**

This URI returns detailed information about the job instance related to the specified job execution.

#### **GET /ibm/api/batch/jobinstances/job instance id/jobexecutions**

This URI returns detailed information about the job execution(s) for a specified job instance. This includes links to associated step executions and job logs.

#### **GET /ibm/api/batch/jobinstances/job instance id/jobexecutions/job execution sequence number**

This URI returns detailed information about the specified job execution in relation to the specified job instance ID. This includes links to associated step executions and job logs.

**Note:** The job execution sequence number means the 0th, 1st, 2nd, etc. job execution related to the specified job instance.

#### **PUT /ibm/api/batch/jobexecutions/job execution id?action=stop**

Use this URI to stop the specified running job execution. Required parameters include action = *stop*, *restart*.

#### **PUT /ibm/api/batch/jobexecutions/job execution id?action=restart**

Use this URI to restart the specified job execution. Required parameters include action = *stop*, *restart*.

## **Step executions**

#### **GET /ibm/api/batch/jobexecutions/job execution id/stepexecutions**

This URI returns a JSON array of all the step execution details for the specified job execution. If your job contains a partitioned step, the partition information will be returned listed within each step.

Sample request:

`https://localhost:8020/ibm/api/batch/jobexecutions/40/stepexecutions`

The following sample illustrates a response for a partitioned step.

```

[
  {
    "stepExecutionId":47,
    "executionId":39,
    "instanceId":35,
    "stepName":"step1",
    "batchStatus":"COMPLETED",
    "startTime":"2015/03/30 11:10:08.652 -0400",
    "endTime":"2015/03/30 11:10:09.817 -0400",
    "exitStatus":"COMPLETED",
    "metrics":{
      "READ_COUNT":"0",
      "WRITE_COUNT":"0",
      "COMMIT_COUNT":"0",
      "ROLLBACK_COUNT":"0",
      "READ_SKIP_COUNT":"0",
      "PROCESS_SKIP_COUNT":"0",
      "FILTER_COUNT":"0",
      "WRITE_SKIP_COUNT":"0"
    },
    "partitions":[
      {
        "partitionNumber":0,
        "batchStatus":"COMPLETED",
        "startTime":"2015/03/30 11:10:09.579 -0400",
        "endTime":"2015/03/30 11:10:09.706 -0400",
        "exitStatus":"step1",
        "metrics":{
          "READ_COUNT":"0",
          "WRITE_COUNT":"0",
          "COMMIT_COUNT":"0",
          "ROLLBACK_COUNT":"0",
          "READ_SKIP_COUNT":"0",
          "PROCESS_SKIP_COUNT":"0",
          "FILTER_COUNT":"0",
          "WRITE_SKIP_COUNT":"0"
        }
      },
      {
        "partitionNumber":1,
        "batchStatus":"COMPLETED",
        "startTime":"2015/03/30 11:10:09.257 -0400",
        "endTime":"2015/03/30 11:10:09.302 -0400",
        "exitStatus":"step1",
        "metrics":{
          "READ_COUNT":"0",
          "WRITE_COUNT":"0",
          "COMMIT_COUNT":"0",
          "ROLLBACK_COUNT":"0",
          "READ_SKIP_COUNT":"0",
          "PROCESS_SKIP_COUNT":"0",
          "FILTER_COUNT":"0",
          "WRITE_SKIP_COUNT":"0"
        }
      },
      {
        "partitionNumber":2,
        "batchStatus":"COMPLETED",
        "startTime":"2015/03/30 11:10:09.469 -0400",
        "endTime":"2015/03/30 11:10:09.548 -0400",
        "exitStatus":"step1",
        "metrics":{
          "READ_COUNT":"0",
          "WRITE_COUNT":"0",
          "COMMIT_COUNT":"0",
          "ROLLBACK_COUNT":"0",
          "READ_SKIP_COUNT":"0",
          "PROCESS_SKIP_COUNT":"0",
          "FILTER_COUNT":"0",
          "WRITE_SKIP_COUNT":"0"
        }
      }
    ]
  }
]

```

```

        "PROCESS_SKIP_COUNT":"0",
        "FILTER_COUNT":"0",
        "WRITE_SKIP_COUNT":"0"
    }
}
]
},
{
    "stepExecutionId":51,
    "executionId":39,
    "instanceId":35,
    "stepName":"step2",
    "batchStatus":"COMPLETED",
    "startTime":"2015/03/30 11:10:09.915 -0400",
    "endTime":"2015/03/30 11:10:10.648 -0400",
    "exitStatus":"COMPLETED",
    "metrics":{
        "READ_COUNT":"0",
        "WRITE_COUNT":"0",
        "COMMIT_COUNT":"0",
        "ROLLBACK_COUNT":"0",
        "READ_SKIP_COUNT":"0",
        "PROCESS_SKIP_COUNT":"0",
        "FILTER_COUNT":"0",
        "WRITE_SKIP_COUNT":"0"
    },
    "partitions":[
        {
            "partitionNumber":0,
            "batchStatus":"COMPLETED",
            "startTime":"2015/03/30 11:10:10.324 -0400",
            "endTime":"2015/03/30 11:10:10.417 -0400",
            "exitStatus":"step2",
            "metrics":{
                "READ_COUNT":"0",
                "WRITE_COUNT":"0",
                "COMMIT_COUNT":"0",
                "ROLLBACK_COUNT":"0",
                "READ_SKIP_COUNT":"0",
                "PROCESS_SKIP_COUNT":"0",
                "FILTER_COUNT":"0",
                "WRITE_SKIP_COUNT":"0"
            }
        },
        {
            "partitionNumber":1,
            "batchStatus":"COMPLETED",
            "startTime":"2015/03/30 11:10:10.260 -0400",
            "endTime":"2015/03/30 11:10:10.347 -0400",
            "exitStatus":"step2",
            "metrics":{
                "READ_COUNT":"0",
                "WRITE_COUNT":"0",
                "COMMIT_COUNT":"0",
                "ROLLBACK_COUNT":"0",
                "READ_SKIP_COUNT":"0",
                "PROCESS_SKIP_COUNT":"0",
                "FILTER_COUNT":"0",
                "WRITE_SKIP_COUNT":"0"
            }
        },
        {
            "partitionNumber":2,
            "batchStatus":"COMPLETED",
            "startTime":"2015/03/30 11:10:10.507 -0400",
            "endTime":"2015/03/30 11:10:10.557 -0400",
            "exitStatus":"step2",

```

```

    "metrics":{
      "READ_COUNT":"0",
      "WRITE_COUNT":"0",
      "COMMIT_COUNT":"0",
      "ROLLBACK_COUNT":"0",
      "READ_SKIP_COUNT":"0",
      "PROCESS_SKIP_COUNT":"0",
      "FILTER_COUNT":"0",
      "WRITE_SKIP_COUNT":"0"
    }
  },
  {
    "_links":[
      {
        "rel":"job execution",
        "href":"https://localhost:9443/ibm/api/batch/jobexecutions/9"
      },
      {
        "rel":"job instance",
        "href":"https://localhost:9443/ibm/api/batch/jobinstances/9"
      }
    ]
  }
]

```

**GET /ibm/api/batch/jobexecutions/job execution id/stepexecutions/step name**

This URI returns a JSON array containing the step execution details for the specified job execution and step name.

**GET /ibm/api/batch/jobinstances/job instance id/jobexecutions/job execution sequence number/stepexecutions/step name**

This URI returns a JSON array containing the step execution details for the specified job instance, job execution, and step name.

**GET /ibm/api/batch/stepexecutions/step execution id**

This URI returns a JSON array containing the step execution details for the specified step execution.

## Job logs

**GET /ibm/api/batch/jobinstances/job instance id/joblogs**

This URI returns a JSON array with REST links to all job log parts for the specified job instance.

**GET /ibm/api/batch/jobexecutions/job execution id/joblogs**

This URI returns a JSON array with REST links to all job log parts for the specified job execution.

**Important:** The following example shows the format of the REST links.

If your job execution has the following job log parts,

```

joblogs/instance.inst-id/execution.exec-id/part.1.log
joblogs/instance.inst-id/execution.exec-id/part.2.log
joblogs/instance.inst-id/execution.exec-id/step.step-name/partition.0/part.1.log
joblogs/instance.inst-id/execution.exec-id/step.step-name/partition.1/part.1.log

```

then the corresponding REST links are:

```

/ibm/api/batch/jobexecutionsexec-id/joblogs?part=part.1.log
/ibm/api/batch/jobexecutionsexec-id/joblogs?part=part.2.log
/ibm/api/batch/jobexecutionsexec-id/joblogs?part=step.step-name/partition.0/part.1.log
/ibm/api/batch/jobexecutionsexec-id/joblogs?part=step.step-name/partition.1/part.1.log

```

Optional parameters include:

**type = text**

Text returns all job logs as plain text. All job log parts are aggregated together. Part delimiting header and footer records are inserted into the stream to delimit the different parts as they are aggregated together.

**type = zip**

Zip returns all job logs for the specified job instance or job execution as a compressed file. The directory structure of the job logs is preserved in the compressed file.

**GET /ibm/api/batch/jobinstances/job instance id/joblogs?type=text | zip**

**GET /ibm/api/batch/jobexecutions/job execution id/joblogs?type=text | zip**

The behavior of these two URIs with the **type** parameter specified varies by value.

**type = text**

Text returns all job logs as plain text. All job log parts are aggregated together. Part delimiting header and footer records are inserted into the stream to delimit the different parts as they are aggregated together.

**type = zip**

Zip returns all job logs for the specified job instance or job execution as a compressed file. The directory structure of the job logs is preserved in the compressed file.

**GET /ibm/api/batch/jobexecutions/job execution id/joblogs?part=path to part&type=text | zip**

With the **part** parameter specified, this URI returns job log parts as either plain text (type=text) or in a compressed file (type=zip). The default setting is type=text.

## HTTP Return Codes

The following HTTP return codes for the REST API.

- HTTP 200 OK
- HTTP 201 Successfully created a new resource.
- HTTP 202 Accepted request, but processing is not complete.
- HTTP 400 Bad Request with invalid parameters. See returned message for details.
- HTTP 401 Unauthorized to access this resource.
- HTTP 403 Authentication failed.
- HTTP 404 The requested resource cannot be found or does not exist.
- HTTP 409 The request conflicts with the current state of the resource. See returned message for details.
- HTTP 500 Internal Server Error.

## STOP requests in a distributed server batch environment

Stop requests sent to the batch REST API must be sent directly to the executor where the job is running. If a stop request is sent to a dispatcher or executor where the job is not running, the request is redirected to the correct executor by an HTTP 302 redirection response message. The **location** field in the HTTP 302 redirection response indicates the correct URL to use for the stop request.

## JOBLOGS requests in a distributed server batch environment

Job logs requests sent to the batch REST API must be sent directly to the executor where the job is running. If a job logs request is sent to a dispatcher or executor where the job is not running, the request is redirected to the correct executor by an HTTP 302 redirection response message. The **location** field in the HTTP 302 redirection response indicates the correct URL to use for the job logs request.

**Note:** Job logs requests that are sent to the batch REST API for an entire job instance work only if all job executions for that instance ran on the same executor. If the executions ran on different executors, then the job logs requests for the instance fails. In this case, you must fetch the job logs for each execution separately.

## Purge requests in a distributed server batch environment

Purge requests sent to the batch REST API must be sent directly to the executor where the job is running. If a purge request is sent to a dispatcher or executor where the job is not running, the request is redirected to the correct executor by an HTTP 302 redirection response message. The **location** field in the HTTP 302 redirection response indicates the correct URL to use for the purge request.

**Note:** Purge requests that are sent to the batch REST API for an entire job instance work only if all job executions for that instance ran on the same executor. If the executions ran on different executors, then the purge requests for the instance fails.

## Enabling multiple server support by using the Liberty embedded messaging provider



8.5.5.6

The batch environment can be set up to have servers function as batch dispatchers while other servers function as batch executors. Batch dispatchers accept requests from external clients and make them available to the batch executors. The batch executors receive requests that match its defined capabilities and execute those requests. Batch dispatchers and batch executors communicate by using Java Messaging Service (JMS).

### Before you begin

Determine where the embedded message engine is hosted. It can be hosted on the batch dispatch server, the batch executor server, or on a separate server. This server must be configured before you complete this task. The JMS connection factory and activation specification references the message engine server in its configuration. To configure the message engine:

1. Add the **wasJmsServer-1.0** feature to the `server.xml`.
2. Define the message engine by adding the **messageEngine** element. Define the queue that is used for the batch dispatcher and batch executor. The following example illustrates the message engine configuration in your `server.xml`.

```
<!--specify the ports for the message engine.
The ports in this example are the default ports.
This element is not needed when the default ports are used. -->
<wasJmsEndpoint host="*"
  wasJmsPort="7280"
  wasJmsSSLPort="7290"
  enabled="true">
</wasJmsEndpoint>

<messagingEngine>
  <!-- queue for batch jms message. -->
  <queue id="batchLibertyQueue"
    forceReliability="ReliablePersistent"
    receiveAllowed="true"/>
</messagingEngine>
```

### About this task

This task helps you configure the batch dispatch server and the batch executor by using the Liberty embedded messaging provider.

## Procedure

To configure batch dispatcher and executor that uses Liberty embedded messaging provider:

1. Configure the batch JMS dispatcher.
  - a. Enable JMS support by adding the **wasJmsClient-2.0** feature to the feature manager in your `server.xml`.
  - b. Add the **batchJmsDispatcher** element to your `server.xml` on the server that hosts the batch dispatcher.

```
<batchJmsDispatcher connectionFactoryRef={reference to a configured JMS connection factory}
queueRef={reference to a configured JMS queue} />
```

**Note:** If you do not specify the `connectionFactoryRef` and `queueRef` attributes, the default value for `connectionFactoryRef` is **batchConnectionFactory** and the default value for `queueRef` is **batchJobSubmissionQueue**. You can specify the `batchJmsDispatcher` element as `<batchJmsDispatcher />`. You still must configure the **batchConnectionFactory** JMS connection factory and the JMS **batchJobSubmissionQueue** queue in the `server.xml` file.

- c. Add the corresponding JMS connection factory and JMS queue to the server configuration. This is not specific to batch configuration. The following example illustrates the batch JMS dispatcher configuration and its JMS configuration.

**Note:** The **remoteServerAddress** attribute points to the `host:port` of the server that is hosting the Liberty message engine.

```
<batchJmsDispatcher connectionFactoryRef="batchConnectionFactory"
queueRef="batchJobSubmissionQueue" />

<jmsConnectionFactory id="batchConnectionFactory"
jndiName="jms/batch/connectionFactory">
  <properties.wasJms remoteServerAddress="host:7280:BootstrapBasicMessaging">
  </properties.wasJms>
</jmsConnectionFactory>

<jmsQueue id="batchJobSubmissionQueue"
jndiName="jms/batch/jobSubmissionQueue">
  <properties.wasJms deliveryMode="Persistent"
queueName="batchLibertyQueue">
  </properties.wasJms>
</jmsQueue>
```

2. Configure the batch JMS executor.
  - a. Enable JMS support by adding the **wasJmsClient-2.0** feature to the feature manager in your `server.xml`.
  - b. Add the **batchJmsExecutor** element to your `server.xml` file on the server that hosts the batch executor.

```
<batchJmsExecutor activationSpecRef={configured activation specification or batch executor}
queueRef={reference to the configured JMS queue} />
```

**Note:** If you do not specify the `activationSpecRef` and `queueRef` attributes, the default value for `activationSpecRef` is **batchActivationSpec** and the default value for `queueRef` is **batchJobSubmissionQueue**. You can specify the `batchJmsExecutor` element as `<batchJmsExecutor />`. You still must configure the JMS activation specification for `batchActivationSpec` and the `batchJobSubmissionQueue` JMS queue in the `server.xml` file.

- c. Add the corresponding JMS activation specification and JMS queue to the server configuration. This is not specific to batch configuration.
  - d. Define batch executor server capabilities by including a JMS message selector in the activation specification.
    - Filtering based on system defined properties:  
There is a set of batch dispatcher properties available on the batch JMS message that the batch executor can use to filter for inbound messages.

- **com\_ibm\_ws\_batch\_applicationName**: the name of the batch application for the job request
- **com\_ibm\_ws\_batch\_moduleName**: the module name of the batch application for the job request
- **com\_ibm\_ws\_batch\_componentName**: the component name of the batch application for the job request

**Note:** It is recommended that a message selector is specified with at least the **com\_ibm\_ws\_batch\_applicationName** property to ensure that the executor only receives jobs that it can process.

The following example indicates the **messageSelector** attribute for the executor to accept a job for the application SimpleBatchJob and BonusPayout.

```
messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob' OR com_ibm_ws_batch_applicationName = 'BonusPayout'>
```

The following example indicates the **messageSelector** attribute for the executor to accept a job for the application SimpleBatchJob.

```
messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob'>
```

- Filtering based on user-defined properties:

The batch dispatcher sets all job parameters that conform to the proper JMS message property on the batch dispatcher request message. These properties can also be used by the message selector to add extra filtering to the message selector. The property name, or identifier, must conform to JMS message property constraints. For example, the property is an unlimited length sequence of letters and digits, the first of which must be a letter. A letter is any character for which the method **Character.isJavaLetter** returns true, and includes '\_' and '\$'. A letter or digit is any character for which the method **Character.isJavaLetterOrDigit** returns true. Check JMS Javadoc for more information on JMS message selectory.

The following example illustrates a possible message selector using the **com\_ibm\_ws\_batch\_applicationName** property and a job parameter **specialCapability**.

```
messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob' AND specialCapability = 'superCapability'>
```

The following example illustrates the batch JMS executor configuration and its JMS configuration.

```
<batchJmsExecutor activationSpecRef="batchActivationSpec"
  queueRef="batchJobSubmissionQueue"/>

<jmsActivationSpec id="batchActivationSpec" >
  <properties.wasJms destinationRef="batchJobSubmissionQueue"
    messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob' OR com_ibm_ws_batch_applicationName = 'BonusPayoutCDI'"
    destinationType="javax.jms.Queue"
    remoteServerAddress="host:7280:BootstrapBasicMessaging">
  </properties.wasJms>
</jmsActivationSpec>

<jmsQueue id="batchJobSubmissionQueue"
  jndiName="jms/batch/jobSubmissionQueue">
  <properties.wasJms deliveryMode="Persistent"
    queueName="batchLibertyQueue">
  </properties.wasJms>
</jmsQueue>
```

3. Install your batch application on the server. For more information, see Chapter 10, “Deploying applications in Liberty,” on page 2139.

## Enabling multiple server support by using the WebSphere MQ messaging provider



8.5.5.6

The batch environment can be set up to have servers function as batch dispatchers while other servers function as batch executors. Batch dispatchers accept requests from external clients and make them available to the batch executors. The batch executors receive requests that match its defined capabilities and execute those requests. Batch dispatchers and batch executors communicate by using Java Messaging Service (JMS).

## About this task

This task helps you configure the batch dispatch server and the batch executor by using the WebSphere MQ messaging provider.

### Procedure

1. Configure the batch JMS dispatcher.
  - a. Enable JMS support by adding the `wmqJmsClient-2.0` feature to the feature manager in your `server.xml` file.
  - b. Add the `batchJmsDispatcher` element to your `server.xml` file on the server that hosts the batch dispatcher.

```
<batchJmsDispatcher connectionFactoryRef={reference to a configured JMS connection factory}  
queueRef={reference to a configured JMS queue} />
```

**Note:** If you do not specify the `connectionFactoryRef` and `queueRef` attributes, the default value for `connectionFactoryRef` is `batchConnectionFactory` and the default value for `queueRef` is `batchJobSubmissionQueue`. You can specify the `batchJmsDispatcher` element as `<batchJmsDispatcher />`. You still must configure the `batchConnectionFactory` JMS connection factory and the JMS `batchJobSubmissionQueue` queue in the `server.xml` file.

- c. Add the corresponding JMS connection factory and JMS queue to the server configuration. This is not specific to batch configuration.

The following example illustrates the batch JMS dispatcher configuration and its JMS configuration using WMQ binding mode.

```
<batchJmsDispatcher connectionFactoryRef="batchConnectionFactory"  
queueRef="batchJobSubmissionQueue" />
```

```
<!-- wmq resource adapter -->  
<variable name="wmqJmsClient.rar.location"  
value="{server.config.dir}/wmq.wlp.rar"/>  
  
<!-- nativeLibraryPath is required for BINDING mode -->  
<!-- the startup retry and reconnect retry properties are  
recommended to ensure robustness of the system.-->  
<wmqJmsClient nativeLibraryPath="/mqm/jms/java/lib"  
startupRetryCount=999  
startupRetryInterval="1000ms"  
reconnectionRetryCount=10  
reconnectionRetryInterval="5m">  
</wmqJmsClient>  
  
<authData password="pwd" user="user">  
</authData>  
  
<jmsConnectionFactory id="batchConnectionFactory"  
jndiName="jms/batch/connectionFactory">  
<properties.wmqJms transportType="BINDINGS"  
queueManager="WMQX">  
</properties.wmqJms>  
</jmsConnectionFactory>  
  
<!-- baseQueueName is the queue defined on WMQ system -->  
<jmsQueue id="batchJobSubmissionQueue"  
jndiName="jms/batch/jobSubmissionQueue">  
<properties.wmqJms baseQueueName="BATCHQ"  
priority="QDEF"  
baseQueueManagerName="WMQX">  
</properties.wmqJms>  
</jmsQueue>
```

The following example illustrates the batch JMS dispatcher configuration and its JMS configuration using WMQ in client mode.

```
<batchJmsDispatcher connectionFactoryRef="batchConnectionFactory"  
queueRef="batchJobSubmissionQueue" />
```

```
<!-- wmq resource adapter -->  
<variable name="wmqJmsClient.rar.location"  
value="{server.config.dir}/wmq.wlp.rar"/>
```

```

<!-- the startup retry and reconnect retry properties are
      recommended to ensure robustness of the system.-->
<wmqJmsClient startupRetryCount=999
  startupRetryInterval="1000ms"
  reconnectionRetryCount=10
  reconnectionRetryInterval="5m">
</wmqJmsClient>

<authData password="pwd" user="user">
</authData>

<jmsConnectionFactory id="batchConnectionFactory"
  jndiName="jms/batch/connectionFactory">
  <properties.wmqJms
    hostname="webs24.pok.stglabs.ibm.com"
    transportType="CLIENT"
    channel="WAS.JMS.SVRCONN"
    port="1414"
    queueManager="WMQX"/>>
</properties.wmqJms>
</jmsConnectionFactory>

<!-- baseQueueName is the queue defined on WMQ system -->
<jmsQueue id="batchJobSubmissionQueue"
  jndiName="jms/batch/jobSubmissionQueue">
  <properties.wmqJms baseQueueName="BATCHQ"
    priority="QDEF"
    baseQueueManagerName="WMQX">
  </properties.wmqJms>
</jmsQueue>

```

## 2. Configure the batch JMS executor.

- a. Enable JMS support by adding the **wmqJmsClient-2.0** feature to the feature manager in your `server.xml` file.
- b. Add the **batchJmsExecutor** element to your `server.xml` file on the server that hosts the batch executor.

```

<batchJmsExecutor activationSpecRef={configured activation specification or batch executor}
  queueRef={reference to the configured JMS queue} />

```

**Note:** If you do not specify the `activationSpecRef` and `queueRef` attributes, the default value for `activationSpecRef` is **batchActivationSpec** and the default value for `queueRef` is **batchJobSubmissionQueue**. You can specify the `batchJmsExecutor` element as `<batchJmsExecutor />`. You still must configure the JMS activation specification for `batchActivationSpec` and the `batchJobSubmissionQueue` JMS queue in the `server.xml` file.

- c. Add the corresponding JMS activation specification and JMS queue to the server configuration. This is not specific to batch configuration.
- d. Define batch executor server capabilities by including a JMS message selector in the activation specification.

- Filtering based on system defined properties:

There is a set of batch dispatcher properties available on the batch JMS message that the batch executor can use to filter for inbound messages.

- **com\_ibm\_ws\_batch\_applicationName:** the name of the batch application for the job request
- **com\_ibm\_ws\_batch\_moduleName:** the module name of the batch application for the job request
- **com\_ibm\_ws\_batch\_componentName:** the component name of the batch application for the job request

**Note:** It is recommended that a message selector is specified with at least the **com\_ibm\_ws\_batch\_applicationName** property to ensure that the executor only receives jobs that it can process.

The following example indicates the **messageSelector** attribute for the executor to accept a job for the application `SimpleBatchJob` and `BonusPayout`.

```

messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob' OR com_ibm_ws_batch_applicationName = 'BonusPayout'">

```

The following example indicates the **messageSelector** attribute for the executor to accept a job for the application SimpleBatchJob.

```
messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob'">
```

- Filtering based on user-defined properties:

The batch dispatcher sets all job parameters that conform to the proper JMS message property on the batch dispatcher request message. These properties can also be used by the message selector to add extra filtering to the message selector. The property name, or identifier, must conform to JMS message property constraints. For example, the property is an unlimited length sequence of letters and digits, the first of which must be a letter. A letter is any character for which the method **Character.isJavaLetter** returns true, and includes '\_' and '\$'. A letter or digit is any character for which the method **Character.isJavaLetterOrDigit** returns true. Check JMS Javadoc for more information on JMS message selectory.

The following example illustrates a possible message selector by using the **com\_ibm\_ws\_batch\_applicationName** property and a job parameter **specialCapability**.

```
messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob' AND specialCapability = 'superCapability'">
```

The following example illustrates the batch JMS executor configuration and its JMS configuration using WMQ binding mode.

```
<batchJmsExecutor activationSpecRef="batchActivationSpec"
  queueRef="batchJobSubmissionQueue"/>

<!-- wmq resource adapter -->
<variable name="wmqJmsClient.rar.location"
  value="${server.config.dir}/wmq.wlp.rar"/>

<!-- nativeLibraryPath is required for BINDING mode -->
<!-- the startup retry and reconnect retry properties are
  recommended to ensure robustness of the system.-->
<wmqJmsClient nativeLibraryPath="/mqm/jms/java/lib"
  startupRetryCount=999
  startupRetryInterval="1000ms"
  reconnectionRetryCount=10
  reconnectionRetryInterval="5m">
</wmqJmsClient>

<authData password="pwd" user="user">
</authData>

<JmsActivationSpec id="batchActivationSpec" >
  <properties.wmqJms destinationRef="batchJobSubmissionQueue"
    destinationType="javax.jms.Queue"
    messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob' OR com_ibm_ws_batch_applicationName = 'BonusPayout'"
    transportType="BINDINGS"
    queueManager="WMQX">
  </properties.wmqJms>
</JmsActivationSpec>

<!-- baseQueueName is the queue defined on WMQ system -->
<jmsQueue id="batchJobSubmissionQueue"
  jndiName="jms/batch/jobSubmissionQueue">
  <properties.wmqJms baseQueueName="BATCHQ"
    priority="QDEF"
    baseQueueManagerName="WMQX">
  </properties.wmqJms>
</jmsQueue>
```

The following example illustrates the batch JMS executor configuration and its JMS configurations using WMQ client mode.

```
<batchJmsExecutor activationSpecRef="batchActivationSpec"
  queueRef="batchJobSubmissionQueue"/>

<!-- wmq resource adapter -->
<variable name="wmqJmsClient.rar.location"
  value="${server.config.dir}/wmq.wlp.rar"/>

<!-- the startup retry and reconnect retry properties are
  recommended to ensure robustness of the system.-->
<wmqJmsClient startupRetryCount=999
  startupRetryInterval="1000ms"
```

```

    reconnectionRetryCount=10
    reconnectionRetryInterval="5m">
</wmqJmsClient>

<authData password="pwd" user="user">
</authData>

<JmsActivationSpec id="batchActivationSpec" >
  <properties.wmqJms destinationRef="batchJobSubmissionQueue"
    messageSelector="com_ibm_ws_batch_applicationName = SimpleBatchJob' OR com_ibm_ws_batch_applicationName = 'BonusPayout'"
    transportType="CLIENT"
    channel="WAS.JMS.SVRCONN"
    destinationType="javax.jms.Queue"
    queueManager="WMQX"
    hostName="webs24.pok.stglabs.ibm.com"
    port="1414">
  </properties.wmqJms>
</jmsActivationSpec>

<!-- baseQueueName is the queue defined on WMQ system -->
<jmsQueue id="batchJobSubmissionQueue"
  jndiName="jms/batch/jobSubmissionQueue">
  <properties.wmqJms baseQueueName="BATCHQ"
    baseQueueManagerName="WMQX">
  </properties.wmqJms>
</jmsQueue>

```

3. Install your batch application on the server. For more information, see Chapter 10, “Deploying applications in Liberty,” on page 2139.

## Enabling multiple server partitions support by using the WebSphere MQ messaging provider

8.5.5.8

You can set up the batch environment to have servers function as batch dispatchers, while other servers function as batch executors.

### About this task

Batch dispatchers accept requests from external clients and make them available to the batch executors. The batch executors receive requests that match its defined capabilities and execute those requests. If the job is configured to run partitions, the batch executors make them available to the other executors to run. The batch executors communicate by using Java Messaging Service (JMS). This task helps you configure the batch dispatch server and the batch executor by using the WebSphere MQ messaging provider.

### Procedure

1. Configure the batch JMS dispatcher.
  - a. Enable JMS support by adding the **wmqJmsClient-2.0** feature to the feature manager in your `server.xml` file.
  - b. Add the **batchJmsDispatcher** element to your `server.xml` file on the server that hosts the batch dispatcher; for example:

```

<batchJmsDispatcher connectionFactoryRef={reference to a configured JMS connection factory}
  queueRef={reference to a configured JMS queue} />

```

**Note:** If you do not specify the `connectionFactoryRef` and `queueRef` attributes, the default value for `connectionFactoryRef` is **batchConnectionFactory** and the default value for `queueRef` is **batchJobSubmissionQueue**. You can specify the `batchJmsDispatcher` element as `<batchJmsDispatcher/>`. You still must configure the **batchConnectionFactory** JMS connection factory and the JMS **batchJobSubmissionQueue** queue in the `server.xml` file.

- c. Add the corresponding JMS connection factory and JMS queue to the server configuration. This is not specific to batch configuration.

The following example illustrates the batch JMS dispatcher configuration and its JMS configuration using WebSphere MQ binding mode:

```
<batchJmsDispatcher connectionFactoryRef="batchConnectionFactory"
  queueRef="batchJobSubmissionQueue" />

<!-- wmq resource adapter -->
<variable name="wmqJmsClient.rar.location"
  value="{server.config.dir}/wmq.wlp.rar"/>

<!-- nativeLibraryPath is required for BINDING mode -->
<!-- the startup retry and reconnect retry properties are
  recommended to ensure robustness of the system.-->
<wmqJmsClient nativeLibraryPath="/mqm/jms/java/lib"
  startupRetryCount=999
  startupRetryInterval="1000ms"
  reconnectionRetryCount=10
  reconnectionRetryInterval="5m">
</wmqJmsClient>

<authData password="pwd" user="user">
</authData>

<jmsConnectionFactory id="batchConnectionFactory"
  jndiName="jms/batch/connectionFactory">
  <properties.wmqJms transportType="BINDINGS"
    queueManager="WMQX">
  </properties.wmqJms>
</jmsConnectionFactory>

<!-- baseQueueName is the queue defined on WMQ system -->
<jmsQueue id="batchJobSubmissionQueue"
  jndiName="jms/batch/jobSubmissionQueue">
  <properties.wmqJms baseQueueName="BATCHQ"
    priority="QDEF"
    baseQueueManagerName="WMQX">
  </properties.wmqJms>
</jmsQueue>
```

The following example illustrates the batch JMS dispatcher configuration and its JMS configuration using WebSphere MQ in client mode:

```
<batchJmsDispatcher connectionFactoryRef="batchConnectionFactory"
  queueRef="batchJobSubmissionQueue" />

<!-- wmq resource adapter -->
<variable name="wmqJmsClient.rar.location"
  value="{server.config.dir}/wmq.wlp.rar"/>

<!-- the startup retry and reconnect retry properties are
  recommended to ensure robustness of the system.-->
<wmqJmsClient startupRetryCount=999
  startupRetryInterval="1000ms"
  reconnectionRetryCount=10
  reconnectionRetryInterval="5m">
</wmqJmsClient>

<authData password="pwd" user="user">
</authData>

<jmsConnectionFactory id="batchConnectionFactory"
  jndiName="jms/batch/connectionFactory">
  <properties.wmqJms
    hostName="webs24.pok.stglabs.ibm.com"
    transportType="CLIENT"
    channel="WAS.JMS.SVRCONN"
    port="1414"
    queueManager="WMQX"/>>
  </properties.wmqJms>
</jmsConnectionFactory>

<!-- baseQueueName is the queue defined on WMQ system -->
<jmsQueue id="batchJobSubmissionQueue"
  jndiName="jms/batch/jobSubmissionQueue">
  <properties.wmqJms baseQueueName="BATCHQ"
    priority="QDEF"
    baseQueueManagerName="WMQX">
  </properties.wmqJms>
</jmsQueue>
```

## 2. Configure the batch JMS executor for executing jobs

- a. Enable JMS support by adding the **wmqJmsClient-2.0** feature to the feature manager in your `server.xml` file.
- b. Add the **batchJmsDispatcher** element to your `server.xml` file on the server that hosts the batch executor.

**Note:** If you do not add the **batchJmsDispatcher** element to your `server.xml` file, the server will not dispatch partitions to run on multiple servers and will run the partitions locally.

- c. Add the **batchJmsExecutor** element and a `connectionFactory` to your `server.xml` file on the server that hosts the batch executor. For more information, see step 1b and 1c.

```
<batchJmsExecutor activationSpecRef={configured activation specification or batch executor}  
queueRef={reference to the configured JMS queue} />
```

**Note:** If you do not specify the `activationSpecRef` and `queueRef` attributes, the default value for `activationSpecRef` is **batchActivationSpec** and the default value for `queueRef` is **batchJobSubmissionQueue**. You can specify the `batchJmsExecutor` element as `<batchJmsExecutor/>`. You still must configure the JMS activation specification for `batchActivationSpec` and the `batchJobSubmissionQueue` JMS queue in the `server.xml` file.

- d. Add the corresponding JMS activation specification and JMS queue to the server configuration. This is not specific to batch configuration.
- e. Define batch executor server capabilities by including a JMS message selector in the activation specification.

- Filter based on system-defined properties:

The following batch dispatcher properties are available on the batch JMS message that the batch executor can use to filter for inbound messages.

- **com\_ibm\_ws\_batch\_applicationName**: the name of the batch application for the job request
- **com\_ibm\_ws\_batch\_moduleName**: the module name of the batch application for the job request
- **com\_ibm\_ws\_batch\_componentName**: the component name of the batch application for the job request
- **com\_ibm\_ws\_batch\_work\_type**: the work type : "Job"

**Note:** Specify a message selector with at least the **com\_ibm\_ws\_batch\_applicationName** property to ensure that the executor only receives jobs that it can process.

The following example indicates the **messageSelector** attribute for the executor to accept a job for the application `SimpleBatchJob` and `BonusPayout`:

```
messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob' OR com_ibm_ws_batch_applicationName = 'BonusPayout'>
```

- Filter based on user-defined properties:

The batch dispatcher sets all job parameters that conform to the proper JMS message property on the batch dispatcher request message. These properties can also be used by the message selector to add extra filtering to the message selector. The property name, or identifier, must conform to JMS message property constraints. For example, the property is an unlimited length sequence of letters and digits, the first of which must be a letter. A letter is any character for which the method **Character.isJavaLetter** returns true, and includes '\_' and '\$'. A letter or digit is any character for which the method **Character.isJavaLetterOrDigit** returns true. Check the JMS API documentation for more information on JMS message selectory.

The following example illustrates a possible message selector by using the **com\_ibm\_ws\_batch\_applicationName** property and a job parameter **specialCapability**:

```
messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob' AND specialCapability = 'superCapability'>
```

The following example illustrates the batch JMS executor configuration and its JMS configuration using WebSphere MQ binding mode:

```

<batchJmsExecutor activationSpecRef="batchActivationSpec"
  queueRef="batchJobSubmissionQueue" />

<!-- wmq resource adapter -->
<variable name="wmqJmsClient.rar.location"
  value="{server.config.dir}/wmq.wlp.rar"/>

<!-- nativeLibraryPath is required for BINDING mode -->
<!-- the startup retry and reconnect retry properties are
  recommended to ensure robustness of the system.-->
<wmqJmsClient nativeLibraryPath="/mqm/jms/java/lib"
  startupRetryCount=999
  startupRetryInterval="1000ms"
  reconnectionRetryCount=10
  reconnectionRetryInterval="5m">
</wmqJmsClient>

<authData password="pwd" user="user">
</authData>

<JmsActivationSpec id="batchActivationSpec" >
  <properties.wmqJms destinationRef="batchJobSubmissionQueue"
    destinationType="javax.jms.Queue"
    messageSelector="(com_ibm_ws_batch_applicationName = 'SimpleBatchJob' OR com_ibm_ws_batch_applicationName = 'BonusPayout') AND com_ibm_ws_batch_applicationName = 'BINDINGS'"
    transportType="BINDINGS"
    queueManager="WMQX">
  </properties.wmqJms>
</JmsActivationSpec>

<!-- baseQueueName is the queue defined on WMQ system -->
<jmsQueue id="batchJobSubmissionQueue"
  jndiName="jms/batch/jobSubmissionQueue">
  <properties.wmqJms baseQueueName="BATCHQ"
    priority="QDEF"
    baseQueueManagerName="WMQX">
  </properties.wmqJms>
</jmsQueue>

```

The following example illustrates the batch JMS executor configuration and its JMS configurations using Websphere MQ client mode:

```

<batchJmsExecutor activationSpecRef="batchActivationSpec"
  queueRef="batchJobSubmissionQueue" />

<!-- wmq resource adapter -->
<variable name="wmqJmsClient.rar.location"
  value="{server.config.dir}/wmq.wlp.rar"/>

<!-- the startup retry and reconnect retry properties are
  recommended to ensure robustness of the system.-->
<wmqJmsClient startupRetryCount=999
  startupRetryInterval="1000ms"
  reconnectionRetryCount=10
  reconnectionRetryInterval="5m">
</wmqJmsClient>

<authData password="pwd" user="user">
</authData>

<JmsActivationSpec id="batchActivationSpec" >
  <properties.wmqJms destinationRef="batchJobSubmissionQueue"
    messageSelector="com_ibm_ws_batch_applicationName = SimpleBatchJob' OR com_ibm_ws_batch_applicationName = 'BonusPayout'"
    transportType="CLIENT"
    channel="WAS.JMS.SVRCONN"
    destinationType="javax.jms.Queue"
    queueManager="WMQX"
    hostName="webs24.pok.stglabs.ibm.com"
    port="1414">
  </properties.wmqJms>
</JmsActivationSpec>

<!-- baseQueueName is the queue defined on WMQ system -->
<jmsQueue id="batchJobSubmissionQueue"
  jndiName="jms/batch/jobSubmissionQueue">
  <properties.wmqJms baseQueueName="BATCHQ"
    baseQueueManagerName="WMQX">
  </properties.wmqJms>
</jmsQueue>

```

3. Configure the batch JMS executor for executing only partitions.
  - a. Enable JMS support by adding the **wmqJmsClient-2.0** feature to the feature manager in your `server.xml` file.
  - b. Add the **batchJmsExecutor** element and a `connectionFactory` to your `server.xml` file on the server that hosts the batch executor. For more information, see step 1b and 1c.

```
<batchJmsExecutor activationSpecRef={configured activation specification or batch executor}
  queueRef={reference to the configured JMS queue}
  replyConnectionFactoryRef={reference to the configured JMS connection factory} />
```

**Note:** If you do not specify the `activationSpecRef` and `queueRef` attributes, the default value for `activationSpecRef` is **batchActivationSpec** and the default value for `queueRef` is **batchJobSubmissionQueue**. You can specify the `batchJmsExecutor` element as `<batchJmsExecutor/>`. You still must configure the JMS activation specification for `batchActivationSpec` and the `batchJobSubmissionQueue` JMS queue in the `server.xml` file.

- c. Add the corresponding JMS activation specification and JMS queue to the server configuration. This is not specific to batch configuration.
- d. Define batch executor server capabilities by including a JMS message selector in the activation specification.

- Filter based on system-defined properties:

The following batch dispatcher properties are available on the batch JMS message that the batch executor can use to filter for inbound messages.

- **com.ibm.ws.batch.applicationName:** the name of the batch application for the job request
- **com.ibm.ws.batch.moduleName:** the module name of the batch application for the job request
- **com.ibm.ws.batch.componentName:** the component name of the batch application for the job request
- **com.ibm.ws.batch.work.type:** the work type : "Partition"
- **com.ibm.ws.batch.partitionNum**(Type=Integer): the partition number of the partition that is being dispatched
- **com.ibm.ws.batch.stepName:** the name of the step as defined in the JSL

**Note:** Specify a message selector with at least the **com.ibm.ws.batch.applicationName** property to ensure that the executor only receives jobs that it can process.

The following example indicates the **messageSelector** attribute for the executor to accept a job for the application `SimpleBatchJob` and `BonusPayout`:

```
messageSelector="com.ibm.ws.batch.applicationName = 'SimpleBatchJob' OR com.ibm.ws.batch.applicationName = 'BonusPayout'>
```

- Filter based on user-defined properties:

The batch dispatcher sets all job parameters that conform to the proper JMS message property on the batch dispatcher request message. These properties can also be used by the message selector to add extra filtering to the message selector. The property name, or identifier, must conform to JMS message property constraints. For example, the property is an unlimited length sequence of letters and digits, the first of which must be a letter. A letter is any character for which the method **Character.isJavaLetter** returns true, and includes '\_' and '\$'. A letter or digit is any character for which the method **Character.isJavaLetterOrDigit** returns true. Check the JMS API documentation for more information on JMS message selector.

The following example illustrates a possible message selector by using the **com.ibm.ws.batch.applicationName** property and a job parameter **specialCapability**:

```
messageSelector="com.ibm.ws.batch.applicationName = 'SimpleBatchJob' AND specialCapability = 'superCapability'>
```

The following example illustrates the batch JMS executor configuration and its JMS configuration using WebSphere MQ binding mode:

```
<jmsConnectionFactory id="batchConnectionFactory"
  jndiName="jms/batch/connectionFactory"/>
```

```
<batchJmsExecutor activationSpecRef="batchActivationSpec"
```

```

        queueRef="batchJobSubmissionQueue"
        replyConnectionFactoryRef="batchConnectionFactory"/>

<!-- wmq resource adapter -->
<variable name="wmqJmsClient.rar.location"
    value="{server.config.dir}/wmq.wlp.rar"/>

<!-- nativeLibraryPath is required for BINDING mode -->
<!-- the startup retry and reconnect retry properties are
    recommended to ensure robustness of the system.-->
<wmqJmsClient nativeLibraryPath="/mqm/jms/java/lib"
    startupRetryCount=999
    startupRetryInterval="1000ms"
    reconnectionRetryCount=10
    reconnectionRetryInterval="5m">
</wmqJmsClient>

<authData password="pwd" user="user">
</authData>

<JmsActivationSpec id="batchActivationSpec" >
    <properties.wmqJms destinationRef="batchJobSubmissionQueue"
        destinationType="javax.jms.Queue"
        messageSelector="(com_ibm_ws_batch_applicationName = 'SimpleBatchJob' OR com_ibm_ws_batch_applicationName = 'BonusPayout') AND com_ibm_ws_batch_applicationName = 'BonusPayout'"
        transportType="BINDINGS"
        queueManager="WMQX">
    </properties.wmqJms>
</jmsActivationSpec>

<!-- baseQueueName is the queue defined on WMQ system -->
<jmsQueue id="batchJobSubmissionQueue"
    jndiName="jms/batch/jobSubmissionQueue">
    <properties.wmqJms baseQueueName="BATCHQ"
        priority="QDEF"
        baseQueueManagerName="WMQX">
    </properties.wmqJms>
</jmsQueue>

```

The following example illustrates the batch JMS executor configuration and its JMS configurations using Websphere MQ client mode:

```

<jmsConnectionFactory id="batchConnectionFactory"
    jndiName="jms/batch/connectionFactory"/>

<batchJmsExecutor activationSpecRef="batchActivationSpec"
    queueRef="batchJobSubmissionQueue"
    replyConnectionFactoryRef="batchConnectionFactory"/>

<!-- wmq resource adapter -->
<variable name="wmqJmsClient.rar.location"
    value="{server.config.dir}/wmq.wlp.rar"/>

<!-- the startup retry and reconnect retry properties are
    recommended to ensure robustness of the system.-->
<wmqJmsClient startupRetryCount=999
    startupRetryInterval="1000ms"
    reconnectionRetryCount=10
    reconnectionRetryInterval="5m">
</wmqJmsClient>

<authData password="pwd" user="user">
</authData>

<JmsActivationSpec id="batchActivationSpec" >
    <properties.wmqJms destinationRef="batchJobSubmissionQueue"
        messageSelector="(com_ibm_ws_batch_applicationName = SimpleBatchJob' OR com_ibm_ws_batch_applicationName = 'BonusPayout') AND com_ibm_ws_batch_applicationName = 'BonusPayout'"
        transportType="CLIENT"
        channel="WAS.JMS.SVRCONN"
        destinationType="javax.jms.Queue"
        queueManager="WMQX"
        hostName="webs24.pok.stglabs.ibm.com"
        port="1414">
    </properties.wmqJms>
</jmsActivationSpec>

<!-- baseQueueName is the queue defined on WMQ system -->
<jmsQueue id="batchJobSubmissionQueue"
    jndiName="jms/batch/jobSubmissionQueue">

```

```

    <properties.wmqJms baseQueueName="BATCHQ"
    baseQueueManagerName="WMQX">
  </properties.wmqJms>
</jmsQueue>

```

4. Install your batch application on the server. For more information, see Chapter 10, “Deploying applications in Liberty,” on page 2139. To disable multiple server partition execution: If you want to have multiple server support but do not want multiple server partition executions, you can set job property `com.ibm.websphere.batch.partition.multiJVM` to `false` in your `jsl` job XML file. The following example illustrates a JSL job to disable multiple server partitions:

```
<property name="com.ibm.websphere.batch.partition.multiJVM" value="false"/>
```

**Note:** If you are running a partition on a remote executor, there are no job logs created for that partition.

## Enabling multiple server partitions support by using the Liberty embedded messaging provider

8.5.5.8

You can set up the batch environment to have servers function as batch dispatchers, while other servers function as batch executors.

### Before you begin

1. Determine where the embedded message engine is hosted. It can be hosted on the batch dispatch server, the batch executor server, or on a separate server. This server must be configured before you complete this task. The JMS connection factory and activation specification references the message engine server in its configuration.
2. To configure the message engine:
  - a. Add the **wasJmsServer-1.0** feature to the `server.xml`.
  - b. Define the message engine by adding the **messageEngine** element. Define the queue that is used for the batch dispatcher and batch executor. The following example illustrates the message engine configuration in your `server.xml` file:

```

<!--specify the ports for the message engine.
The ports in this example are the default ports.
This element is not needed when the default ports are used. -->
<wasJmsEndpoint host="*"
  wasJmsPort="7280"
  wasJmsSSLPort="7290"
  enabled="true">
</wasJmsEndpoint>

<messagingEngine>
  <!-- queue for batch jms message. -->
  <queue id="batchLibertyQueue"
    forceReliability="ReliablePersistent"
    receiveAllowed="true"/>
</messagingEngine>

```

### About this task

Batch dispatchers accept requests from external clients and make them available to the batch executors. The batch executors receive requests that match its defined capabilities and execute those requests. If the job is configured to run partitions, the batch executors make them available to the other executors to run. The batch executors communicate with each other by using Java Messaging Service (JMS). This task helps you configure the batch dispatch server and the batch executor by using the Liberty profile embedded messaging provider.

### Procedure

1. Configure the batch JMS dispatcher.

- a. Enable JMS support by adding the **wasJmsClient-2.0** feature to the feature manager in your `server.xml` file.
- b. Add the **batchJmsDispatcher** element to your `server.xml` file on the server that hosts the batch dispatcher; for example:

```
<batchJmsDispatcher connectionFactoryRef={reference to a configured JMS connection factory}
queueRef={reference to a configured JMS queue} />
```

**Note:** If you do not specify the `connectionFactoryRef` and `queueRef` attributes, the default value for `connectionFactoryRef` is **batchConnectionFactory** and the default value for `queueRef` is **batchJobSubmissionQueue**. You can specify the `batchJmsDispatcher` element as `<batchJmsDispatcher/>`. You still must configure the **batchConnectionFactory** JMS connection factory and the JMS **batchJobSubmissionQueue** queue in the `server.xml` file.

- c. Add the corresponding JMS connection factory and JMS queue to the server configuration. This is not specific to batch configuration. The following example illustrates the batch JMS dispatcher configuration and its JMS configuration:

**Note:** The `remoteServerAddress` attribute points to the `host:port` of the server that is hosting the Liberty profile message engine.

```
<batchJmsDispatcher connectionFactoryRef="batchConnectionFactory"
queueRef="batchJobSubmissionQueue" />

<jmsConnectionFactory id="batchConnectionFactory"
jndiName="jms/batch/connectionFactory">
  <properties.wasJms remoteServerAddress="host:7280:BootstrapBasicMessaging">
  </properties.wasJms>
</jmsConnectionFactory>

<jmsQueue id="batchJobSubmissionQueue"
jndiName="jms/batch/jobSubmissionQueue">
  <properties.wasJms deliveryMode="Persistent"
queuename="batchLibertyQueue">
  </properties.wasJms>
</jmsQueue>
```

## 2. Configure the batch JMS executor for executing batch jobs.

- a. Enable JMS support by adding the **wasJmsClient-2.0** feature to the feature manager in your `server.xml` file.
- b. Add the **batchJmsDispatcher** element to your `server.xml` file on the server that hosts the batch executor.

```
<batchJmsExecutor activationSpecRef={configured activation specification or batch executor}
queueRef={reference to the configured JMS queue} />
```

**Note:** If you do not add the **batchJmsDispatcher** element to your `server.xml` file, the server will not dispatch partitions to run on multiple servers and will run the partitions locally.

**Note:** If you do not specify the `connectionFactoryRef` and `queueRef` attributes, the default value for `connectionFactoryRef` is **batchConnectionFactory** and the default value for `queueRef` is **batchJobSubmissionQueue**. You can specify the `batchJmsDispatcher` element as `<batchJmsDispatcher/>`. You still must configure the **batchConnectionFactory** JMS connections factory and the `batchJobSubmissionQueue` in the `server.xml` file.

- c. Add the corresponding JMS connection factory and JMS queue to the server configuration. This is not specific to batch configuration. The following example illustrates the batch JMS dispatcher configuration and its JMS configuration:

**Note:** The `remoteServerAddress` attribute points to the `host:port` of the server that is hosting the Liberty profile message engine.

```
<batchJmsDispatcher connectionFactoryRef="batchConnectionFactory"
queueRef="batchJobSubmissionQueue" />

<jmsConnectionFactory id="batchConnectionFactory"
jndiName="jms/batch/connectionFactory">
```

```

<properties.wasJms remoteServerAddress="host:7280:BootstrapBasicMessaging">
</properties.wasJms>
</jmsConnectionFactory>

<jmsQueue id='batchJobSubmissionQueue'
  jndiName="jms/batch/jobSubmissionQueue">
  <properties.wasJms deliveryMode="Persistent"
    queueName="batchLibertyQueue">
  </properties.wasJms>
</jmsQueue>

```

- d. Add the **batchJmsExecutor** element to your **server.xml** on the server that hosts the batch executor; for example:

```

<batchJmsExecutor activationSpecRef={configured activation specification or batch executor}
  queueRef={reference to the configured JMS queue} />

```

**Note:** If you do not specify the `activationSpecRef` and `queueRef` attributes, the default value for `activationSpecRef` is **batchConnectionFactory** and the default value for `queueRef` is **batchJobSubmissionQueue**. You can specify the `batchJmsExecutor` element as `<batchJmsExecutor/>`. You still must configure the JMS activation specification for **batchActivationSpec** and the **batchJobSubmissionQueue** queue in the `server.xml` file.

- e. Add the corresponding JMS activation specification and JMS queue to the server configuration. This is not specific to batch configuration.
- f. Define batch executor server capabilities by including a JMS message selector in the activation specification.

- Filter based on system-defined properties:

The following batch dispatcher properties are available on the batch JMS message that the batch executor can use to filter for inbound messages.

- **com\_ibm\_ws\_batch\_applicationName:** the name of the batch application for the job request
- **com\_ibm\_ws\_batch\_moduleName:** the module name of the batch application for the job request
- **com\_ibm\_ws\_batch\_componentName:** the component name of the batch application for the job request
- **com\_ibm\_ws\_batch\_work\_type:** the work type : "Job"

**Note:** Specify a message selector with at least the **com\_ibm\_ws\_batch\_applicationName** property to ensure that the executor only receives jobs that it can process.

The following example indicates the **messageSelector** attribute for the executor to accept only batch jobs for the application `SimpleBatchJob`:

```
messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob' AND com_ibm_ws_batch_work_type = 'Job'">
```

- Filtering based on user-defined properties:

The batch dispatcher sets all job parameters that conform to the proper JMS message property on the batch dispatcher request message. These properties can also be used by the message selector to add extra filtering to the message selector. The property name, or identifier, must conform to JMS message property constraints. For example, the property is an unlimited length sequence of letters and digits, the first of which must be a letter. A letter is any character for which the method `Character.isJavaLetter` returns true, and includes '\_' and '\$'. A letter or digit is any character for which the method `Character.isJavaLetterOrDigit` returns true. Check the JMS API documentation for more information on JMS message selector.

The following example illustrates a possible message selector by using the **com\_ibm\_ws\_batch\_applicationName** property and a job parameter **specialCapability**:

```
messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob' AND specialCapability = 'superCapability'">
```

The following example illustrates the batch JMS executor configuration and its JMS configuration:

```

<batchJmsExecutor activationSpecRef="batchActivationSpec"
  queueRef="batchJobSubmissionQueue"/>

<jmsActivationSpec id="batchActivationSpec" >
  <properties.wasJms destinationRef="batchJobSubmissionQueue"

```



sequence of letters and digits, the first of which must be a letter. A letter is any character for which the method `Character.isJavaLetter` returns true, and includes '\_' and '\$'. A letter or digit is any character for which the method `Character.isJavaLetterOrDigit` returns true. Check the JMS API documentation for more information on JMS message selectory.

The following example illustrates a possible message selector by using the `com_ibm_ws_batch_applicationName` property and a job parameter `specialCapability`:

```
messageSelector="com_ibm_ws_batch_applicationName = 'SimpleBatchJob' AND specialCapability = 'superCapability'">
```

The following example illustrates the batch JMS executor configuration and its JMS configuration:

```
<jmsConnectionFactory id="batchConnectionFactory"
    jndiName="jms/batch/connectionFactory"/>

<batchJmsExecutor activationSpecRef="batchActivationSpec"
    queueRef="batchJobSubmissionQueue"
    replyConnectionFactoryRef="batchConnectionFactory"/>

<jmsActivationSpec id="batchActivationSpec" >
  <properties.wasJms destinationRef="batchJobSubmissionQueue"
    messageSelector="(com_ibm_ws_batch_applicationName = 'SimpleBatchJob' OR com_ibm_ws_batch_applicationName = 'BonusPayoutCDI') AND com_ibm_ws_batch_applicationName = 'SimpleBatchJob'"
    destinationRef="batchJobSubmissionQueue"
    destinationType="javax.jms.Queue"
    remoteServerAddress="host:7280:BootstrapBasicMessaging">
  </properties.wasJms>
</jmsActivationSpec>

<jmsQueue id="batchJobSubmissionQueue"
    jndiName="jms/batch/jobSubmissionQueue">
  <properties.wasJms deliveryMode="Persistent"
    queueName="batchLibertyQueue">
  </properties.wasJms>
</jmsQueue>
```

4. Install your batch application on the server. For more information, see Chapter 10, “Deploying applications in Liberty,” on page 2139. To disable multiple server partition execution: If you want to have multiple server support but do not want multiple server partition executions, you can set job property `com.ibm.websphere.batch.partition.multiJVM` to false in your jsl job XML file. The following example illustrates a JSL job to disable multiple server partitions:

```
<property name="com.ibm.websphere.batch.partition.multiJVM" value="false"/>
```

**Note:** If you are running a partition on a remote executor, there are no job logs created for that partition.

## Enabling batch job events publishing

8.5.5.7

By using Java Messaging System (JMS), the batch server can publish job-related events to external clients.

### About this task

The ability of the batch server to publish job-related events to external clients enables a monitor to see job-related events and report on failures. The batch dispatcher server can publish events for a job in the dispatching phase. The batch executor server can publish events for jobs when it moves through different phases of execution. These events are published in a topic tree in the following structures:

Table 176. File structures of topic trees for event publishing

Structure	Description
batch	The root of the topic tree.
batch/jobs	The topic tree for all job-related events.
batch/jobs/instance	The topic tree for all events that are related to a job instance.

Table 176. File structures of topic trees for event publishing (continued)

Structure	Description
batch/jobs/instance/submitted	A topic tree node. A message is published when the batch server creates a job instance for a new job submission.
batch/jobs/instance/jms_queued	A topic tree node. A message is published when job submission is placed on the job submission queue by the batch JMS dispatcher.
batch/jobs/instance/jms_consumed	A topic tree node. A message is published when the batch executor receives the job submission from the job submission queue.
batch/jobs/instance/dispatched	A topic tree node. A message is published when the batch executor accepts a job instance for execution.
batch/jobs/instance/completed	A topic tree node. A message is published when the job instance is completed.
batch/jobs/instance/stopped	A topic tree node. A message is published when the job instance is stopped.
batch/jobs/instance/stopping	A topic tree node. A message is published when the job instance is stopping.
batch/jobs/instance/failed	A topic tree node. A message is published when the job instance failed.
batch/jobs/instance/purged	A topic tree node. A message is published when a job instance is purged successfully.
batch/jobs/execution	The topic tree for all events that are related to a job execution.
batch/jobs/execution/restarting	A topic tree node. A message is published when the batch executor is restarting an execution.
batch/jobs/execution/starting	A topic tree node. A message is published when a job execution is starting.
batch/jobs/execution/completed	A topic tree node. A message is published when a job execution ends successfully.
batch/jobs/execution/failed	A topic tree node. A message is published when a job execution ends because of failure.
batch/jobs/execution/stopped	A topic tree node. A message is published when a job execution is stopped.
batch/jobs/execution/jobLogPart	A topic tree node. A message is published when a new job log part is created, a job stops, or a job ends.
batch/jobs/execution/step/started	A topic tree node. A message is published when a step execution is started.
batch/jobs/execution/step/completed	A topic tree node. A message is published when a step execution is completed successfully.
batch/jobs/execution/step/failed	A topic tree node. A message is published when a step execution fails.
batch/jobs/execution/step/stopped	A topic tree node. A message is published when a step execution is stopped.

Table 176. File structures of topic trees for event publishing (continued)

Structure	Description
batch/jobs/execution/step/checkpoint	A topic tree node. A message is published when a checkpoint is taken.
batch/jobs/execution/partition/started	A topic tree node. A message is published when a partition is started.
batch/jobs/execution/partition/completed	A topic tree node. A message is published when a partition is completed successfully.
batch/jobs/execution/partition/failed	A topic tree node. A message is published when a partition fails.
batch/jobs/execution/partition/stopped	A topic tree node. A message is published when a partition is stopped.
batch/jobs/execution/split-flow/started	A topic tree node. A message is published when a split-flow is started.
batch/jobs/execution/split-flow/ended	A topic tree node. A message is published when a split-flow is completed.

The published message for each topic is a JMS TextMessage. The contents of this message is a JSON formatted string that represents the object of the topic, such as job instance, job execution, step execution, or partition. In addition, this message also includes the following JMS message properties set:

- com\_ibm\_ws\_batch\_internal\_jobInstanceId: The job instance ID, if available.
- com\_ibm\_ws\_batch\_internal\_jobExecutionId: The job execution ID, if available.
- com\_ibm\_ws\_batch\_internal\_stepExecutionId: The job step execution ID, if available.

The batch server must be configured to enable the publishing of job-related events. The batch dispatcher and batch executor have the same configuration. The following steps enable the publication of job-related events for a batch server.

## Procedure

1. Enable JMS support by adding the appropriate JMS feature to the feature manager in the server.xml file. If you are using the WebSphere Application Server Liberty default messaging provider, add the **wasJmsClient-2.0** feature and related JMS configurations for the message engine. If you are using WebSphere MQ Messaging provider, add the **wmqJmsClient-2.0** feature.

2. Add the **batchJmsEvents** element to the server.xml file.

```
<batchJmsEvents connectionFactoryRef="batchConnectionFactory" />
```

**Note:** If you do not specify the **connectionFactoryRef** attribute, the default value for **connectionFactoryRef** is **batchConnectionFactory**. You must still configure the **batchConnectionFactory** JMS connection factory in the server.xml file.

3. Add the corresponding JMS connection factory to the server configuration. This is not specific to batch configuration.

The following example illustrates the batch events configuration and its JMS configuration by using the WebSphere MQ messaging provider.

```
<!-- wmq resource adapter -->
<variable name="wmqJmsClient.rar.location" value="{server.config.dir}/wmq.wlp.rar"/>
<!-- require for BINDING mode -->
<wmqJmsClient nativeLibraryPath="/mqm/jms/java/lib"/>

<batchJmsEvents connectionFactoryRef="batchConnectionFactory" />
```

```
<jmsConnectionFactory id="batchConnectionFactory" jndiName="jms/batch/connectionFactory">
  <properties.wmq.Jms
    transportType="BINDINGS"
    queueManager="WMQX" />
</jmsConnectionFactory>
```

The following example illustrates the batch events configuration and its JMS configuration by using the WebSphere Liberty default messaging provider.

```
<batchJmsEvents connectionFactoryRef="batchConnectionFactory" />
<jmsConnectionFactory id="batchConnectionFactory" jndiName="jms/batch/connectionFactory">
  <properties.wasJms></properties.wasJms>
</jmsConnectionFactory>
```

## Example

The following examples illustrate sequence of events for basic execution flows.

- Submit and run a single-step job with checkpoints.

```
batch/jobs/instance/submitted
batch/jobs/instance/jms_queued
batch/jobs/instance/jms_consumed
batch/jobs/execution/starting
batch/jobs/instance/dispatched
batch/jobs/execution/started
batch/jobs/execution/step/started
batch/jobs/execution/step/checkpoint
batch/jobs/execution/step/checkpoint
...
batch/jobs/execution/step/checkpoint
batch/jobs/execution/step/completed
batch/jobs/execution/completed
batch/jobs/instance/completed
```

- Submit and run a single-step job with partition.

```
batch/jobs/instance/submitted
batch/jobs/instance/jms_queued
batch/jobs/instance/jms_consumed
batch/jobs/execution/starting
batch/jobs/instance/dispatched
batch/jobs/execution/started
batch/jobs/execution/step/started
batch/jobs/execution/partition/started
batch/jobs/execution/partition/started
batch/jobs/execution/partition/started
batch/jobs/execution/partition/completed
batch/jobs/execution/partition/completed
batch/jobs/execution/partition/completed
batch/jobs/execution/step/completed
batch/jobs/execution/completed
batch/jobs/instance/completed
```

## batchManager command-line client utility



8.5.5.6

The batchManager command-line client utility provides a command-line interface for managing your batch jobs that run on Liberty.

The batchManager command-line client utility interacts with the batch manager over the batch manager's REST API. To use the batchManager command-line client utility, the batch manager must be running on your Liberty server. Use the batch management feature to install and enable the Liberty batch manager.

## SSL configuration

The batchManager command-line client utility communicates with the batch manager over an SSL connection. To facilitate SSL communication with a batch manager that is running on a Liberty server, the utility must be able to verify the SSL certificate of the Liberty server.

If the SSL certificate is signed by a well-known certificate authority (CA), the utility can verify the certificate by the CA. No further configuration is necessary.

If the SSL certificate is not signed by a CA, then you must configure the utility to trust the SSL certificate of the server by doing one of the following actions.

- Specify the option `--trustSslCertificates`, which configures the utility to trust all SSL certificates.
- Include the server's SSL certificate in the utility's truststore.

If you choose to specify the option `--trustSslCertificates`, the utility trusts all SSL certificates that it receives and no further configuration is necessary.

If you choose the option to include the server's SSL certificate in the utility's truststore, then you must also configure the utility so that it can find its truststore. The utility is a stand-alone Java main. You configure SSL by using system properties such as `javax.net.ssl.truststore`.

If the batch manager is running on the same machine as the utility, then you can point the utility directly at the server keystore:

```
$ export JVM_ARGS="-Djavax.net.ssl.trustStore=/path/to/server/keystore.jks"
$ batchManager submit ...
```

**Attention:** JVM arguments, such as `-D` properties, are passed to the batchManager command-line client utility by the `JVM-ARGS` environment variable.

If you cannot use the server keystore directly, you must export the server certificate from the server keystore and import it into the client truststore. Use the JDK keytool utility for exporting and importing certificates. In the following example, the server certificate is stored in the `[server-dir]/resources/security/key.jks` keystore file under the `default` alias, and the password is `Liberty`.

```
$ keytool -export -alias default -file server.crt -keystore [server-dir]/resources/security/key.jks -storepass Liberty
$ keytool -import -alias server_cert -file server.crt -keystore /path/to/truststore.jks -storepass password
```

**Attention:** The `import` command creates the `truststore.jks` file if the file does not exist.

```
$ export JVM_ARGS="-Djavax.net.ssl.trustStore=/path/to/truststore.jks"
$ batchManager submit ...
```

## Commands and usage

The batchManager command-line client utility provides commands for submitting, stopping, restarting, and checking the status of jobs.

To generally use the utility:

```
$ batchManager [command] [options]
```

To see a list of available commands:

```
$ batchManager help
```

To see the description and options for a specific command:

```
$ batchManager help [command]
```

The following example illustrates how to submit a job and wait for its completion:

```
$ batchManager submit \  
  --batchManager=<host>:<port>  
  --user=[credentials for logging into the batch manager]  
  --password=[credentials for logging into the batch manager]  
  --applicationName=[application name used when packaging the batch app]  
  --jobXMLName=[job XML file basename in the app's batch-jobs dir]  
  --wait
```

## jobParametersFile and jobPropertiesFile

When submitting a batch job by using the batchManagerZos client utility, the jobParametersFile and jobPropertiesFiles supports the use of multiple files separated by commas. Files later in the comma separated list take precedence over files that appear first in the list. The following example illustrates correct usage of the comma separated list.

```
jobParametersFile=filePath1,filePath2,filePath3  
jobPropertiesFile=filePath1,filePath2,filePath3
```

As an example, `--jobParametersFile=<filepath1>` would override `--jobParametersFile=<filepath1>,<filepath2>` in the control properties file. The resulting parameter is `--jobParametersFile=<filepath1>`.

z/OS

## batchManager command-line client utility on z/OS with an SAF key ring

To use the System Authorization Facility (SAF) key ring of your WebSphere Application Server Liberty server with the batchManager command-line client utility, you must set the java.environment settings and a user ID specified on the batchManager command-line client utility call that is authorized to read the SAF key ring.

The following commands authorize the user to read the SAF key ring.

**Important:** The *ringOwnerId* is normally the same ID as the user ID of the WebSphere Application Server Liberty server.

```
PermitRingOwnerId.RingName.LST CLASS(RDATALIB) ID(userId) ACCESS(UPDATE)
```

```
SETROPTS RACLIST(RDATALIB) GENERIC(RDATALIB) REFRESH
```

For more information, see the WebSphere Application Server z/OS Security Server RACF command language reference.

The following example defines the environment variable JVM\_ARGS.

```
export JVM_ARGS="-Djavax.net.ssl.trustStore=safkeyring://ringOwnerId/ringName  
-Djavax.net.ssl.trustStoreType=JCERACFKS -Djavax.net.ssl.keyStore=safkeyring://ringOwnerId/ringName  
-Djavax.net.ssl.keyStoreType=JCERACFKS -Dcom.ibm.ssl.keyStoreFileBased=false -Dcom.ibm.ssl.trustStoreFileBased=false  
-Djava.protocol.handler.pkgs=com.ibm.crypto.provider -Djavax.net.ssl.keyStorePassword=password"
```

**Attention:** The `javax.net.ssl.keyStorePassword` property is required and its value must be password and is used for decoding the copy of the key information in the Java virtual machine (JVM) while it exists in storage.

## Return codes

The batchManager command-line client utility outputs the following return codes:

Code	Description
0	The task completed normally.
20	A required argument was not specified.
21	An unrecognized argument was specified.
22	An invalid argument value was specified.
255	An unknown error occurred.

**Note:** If you specify the `--wait` argument, the utility outputs the following return codes about the status of the job that you are waiting for.

Code	Description
33	The job stopped.
34	The job did not complete successfully.
35	The job completed successfully.
36	The job was abandoned.

## Configuring the batchManagerZos client utility



You can manage batch jobs that are running on Liberty on z/OS by using the batchManagerZos client utility.

### About this task

The batchManagerZos client utility is a natively compiled version of the batchManager command-line utility for managing batch jobs that are running on Liberty for z/OS. It is a native program and does not require a JVM. The utility is included with the batchManagement-1.0 feature.

The batchManagerZos client utility supports a subset of the commands and options that are supported by the batchManager command-line utility. Use the `$ batchManagerZos help` command to view the list of commands and options.

The batchManagerZos client utility uses optimized local adapters to connect to a Liberty server that is running in a local environment. The batchManagerZos client utility cannot connect to remote servers.

### Security Considerations

The security behavior of the batchManagerZos client utility depends on whether the Liberty server uses a SAF registry.

- If the server is using a SAF user registry, then the batchManagerZos client utility identity is set as the requestor's identity (the JEE RunAs Subject) for the batch request.
- If the server is not using a SAF user registry, then the batchManagerZos client utility identity is ignored. In this case, the EVERYONE special subject is set as the requestor's identity for the batch request.

### Batch role-based authorization

If appSecurity is enabled in the server, you must assign the requestor's identity to the appropriate batch security role required by the request. Valid batch security roles are batchAdmin, batchSubmitter and batchMonitor. If the identity is not assigned to the role that is required, the request fails with a security exception.

Authorization is managed by the security authorization provider. If the server using SAF authorization, the SAF authorization provider determines the authorization of the requestor's identity by checking the identity's access to SAF resource profiles defined the EJBROLE class. By default, the following resource profiles are associated with the batch roles.

```
batchAdmin:      BBGZDFLT.com.ibm.ws.batch.batchAdmin
batchSubmitter: BBGZDFLT.com.ibm.ws.batch.batchSubmitter
batchMonitor:   BBGZDFLT.com.ibm.ws.batch.batchMonitor
```

The requestor's identity must be granted READ access to the appropriate resource profile to be authorized to the corresponding batch role.

The following example illustrates the RACF commands to grant the client identity, bob, authorization to the batchAdmin role.

```
RDEFINE EJBROLE BBGZDFLT.com.ibm.ws.batch.batchAdmin UACC(NONE)
PERMIT BBGZDFLT.com.ibm.ws.batch.batchAdmin CLASS(EJBROLE) ID(bob) ACCESS(READ)
```

### | jobParametersFile and jobPropertiesFile

| When submitting a batch job by using the batchManagerZos client utility, the jobParametersFile and jobPropertiesFiles supports the use of multiple files separated by commas. Files later in the comma separated list take precedence over files that appear first in the list. The following example illustrates correct usage of the comma separated list.

```
| jobParametersFile=filePath1,filePath2,filePath3
| jobPropertiesFile=filePath1,filePath2,filePath3
```

| As an example, `--jobParametersFile=<filepath1>` would override `--jobParametersFile=<filepath1>,<filepath2>` in the control properties file. The resulting parameter is `--jobParametersFile=<filepath1>`.

### Job Log streaming

The client subscribes to job log events and prints the received message to the **STDOUT** if the `--getJobLog`, `--queueManagerName`, and `--wait` command options are specified on the **submit** or **restart** command. To receive job log events, batch job events publishing must be enabled. For more information about configuring batch job events publishing, see *Enabling batch job events publishing*.

### Return codes

The batchManagerZos client utility outputs the following return codes:

Code	Description
0	The task completed normally.
20	A required argument was not specified.
21	An unrecognized argument was specified.
22	An invalid argument value was specified.
255	An unknown error occurred.

**Note:** If you specify the `--wait` argument, the utility outputs the following return codes about the status of the job that you are waiting for.

Code	Description
33	The job stopped.
34	The job did not complete successfully.
35	The job completed successfully.
36	The job was abandoned.

**Note:** If you run `batchManagerZos` by running `BPXBATCH`, the return code from `BPXBATCH` will not match the return code from `batchManagerZos`. `BPXBATCH` takes the `batchManagerZos` return code and shifts it up by one byte. For example, if `batchManagerZos` returns 1, then `BPXBATCH` returns 256, which is the hex value `0x01`, shifted up one byte to `0x100`.

If you call `BPXBATCH` from a JCL STEP, the STEP return code is truncated to the lower three hex characters of the return code from `BPXBATCH`. For example, if `batchManagerZos` returns 35, which is `0x23` hex, the `BPXBATCH` will return `0x2300`. The JCL STEP truncates the return code to `0x0300`, or 768.

### Limitations

The `batchManagerZos` client utility **stop** commands must be directed at the batch executor where the job is running. **Stop** commands in a multi-server environment might fail with a `BatchJobNotLocalException` if the `batchManagerZos` client utility connects to a designated batch dispatcher rather than the batch executor where the job is running. Batch dispatchers typically receive submission requests and distribute them to downstream batch executors.

### Procedure

1. Enable the `batchManagement-1.0` and `zosLocalAdapters-1.0` features in your `server.xml` file.

```
<featureManager>
  <feature>batchManagement-1.0</feature>
  <feature>zosLocalAdapters-1.0</feature>
</featureManager>
```

2. Configure a `zosLocalAdapters-1.0` endpoint. The following example illustrates a `zosLocalAdapters-1.0` endpoint configuration.

```
<zosLocalAdapters wolaGroup="LIBERTY" wolaName2="BATCH" wolaName3="MANAGER"/>
```

3. Permit the `batchManagerZos` client utility to connect to the `zosLocalAdapters` endpoint. For the `batchManagerZos` client to connect to the server over optimized local adapters, the `userId` of the client must be authorized to the CBIND SAF resource associated with the `zosLocalAdapters` endpoint. The resource that is associated with the endpoint is named `BBG.WOLA.{wolaGroup}.{wolaName2}.{wolaName3}` in the CBIND class. To bind the `zosLocalAdapters` endpoint that is named `LIBERTY BATCH MANAGER`, you must grant read access to resource `BBG.WOLA.LIBERTY.BATCH.MANAGER` in class `CBIND` for the `batchManagerZos` `userId`. The following example illustrates the RACF commands that you must use to grant read access to the resource.

```
RDEFINE CBIND BBG.WOLA.LIBERTY.BATCH.MANAGER UACC(NONE)
PERMIT BBG.WOLA.LIBERTY.BATCH.MANAGER CLASS(CBIND) ACCESS(READ) ID(bob)
```

**Note:** In this example, `bob` is the user that is running `batchManagerZos`.

4. If you want `batchManagerZos` requests to run on the server under the client's identity, you must authorize the server to use SAFCREDS z/OS authorized resources. The following example illustrates the RACF commands that you must use to enable the server to use SAFCREDS z/OS authorized resources.

```
RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.SAFCREDS UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.SAFCREDS CLASS(SERVER) ACCESS(READ) ID(wluser1)
```

5. Start the Angel address space.
6. Start the Liberty server.

7. Use the **ping** command to test connectivity between the batchManagerZos client and the Liberty server.

```
$ batchManagerZos ping '--batchManager=LIBERTY BATCH MANAGER'
```

If the ping was successful, the client exits with a return code of 0. If the ping was not successful, an error message is issued.

8. To troubleshoot, you can enable extra tracing in the client by setting the `$ export batchManagerZosTrace=1` environment variable.
9. Optional: Configure the batchManagerZos client utility to wait for a batch job event to exit, instead of waiting by using polling.

You must configure the batch server to enable the publishing of job-related events that use WebSphere MQ messaging provider. See the documentation for Enabling batch job events publishing

The following example shows how to submit a job and wait for its completion by a job end event:

```
$ batchManagerZos submit
--batchManager=LIBERTY+BATCH+MANAGER
--applicationName=[application name used when
    packaging the batch app]
--jobXMLName=[job XML file basename in the app's batch-jobs dir]
--wait
--queueManagerName=[name of MQ queue manager]
```

The batchManagerZos client waits to receive 1 of 3 events that represents a job instance ended state:

```
batch/jobs/instance/stopped
batch/jobs/instance/failed
batch/jobs/instance/completed
```

## Viewing Java batch job logs



8.5.5.6

When you are running Java batch jobs in the WebSphere Application Server Liberty, a log is written for each job.

The logs are created in the following directory structure:

```
log directory/joblogs/job name/date/instance.job instance ID/execution.execution ID
```

**Attention:** The variable *job name* is the *id* attribute of the job element within the JSL (XML) document. It is not necessarily related to the file name of the JSL file.

The naming of logs begins at `part.1.log` and rotates to new log parts as needed. By default, the job log contains all messages and trace information that is logged in the server by the thread that performs the job execution. Output that is not logged within the `java.util.logging` framework is not collected.

**Important:** If a new log part cannot be created, batch attempts to continue processing without a log, or with the current log part.

For more information about retrieving or deleting job logs by using the REST API, see the *REST API administration* documentation.

**Important:** If you use the `log4j` API, applications that use the `log4j` framework can participate in batch job logging by using `org.apache.log4j.jul.JULAppender`. The `JULAppender` forwards `log4j` log records to the `java.util.logging` framework, where they are collected for job logging.

## Configuring job logging

Batch job logging can be configured by using the `<batchJobLogging>` configuration element `<batchJobLogging enabled="true" maxRecords="1000" />`.

The attribute `maxRecords` indicates the number of records that are written to a job log part before the records roll over to the next part.

The batch feature uses a logger that is named `com.ibm.ws.batch.JobLogger` to log certain batch messages to the job log only. Examples include job lifecycle messages and checkpoint messages. The logger does not write to the server log. By default, the logger is enabled for Level `.FINE` messages. You can configure the level of the logger by specifying it in the trace specification of the server. For example, `<logging traceSpecification="*=info:com.ibm.ws.batch.JobLogger=all" />`.

Any log messages that are written by the job thread, including messages that are written by the run time and by application code, are written to both the job log and the server log.

The `System.out` and `System.err` files are only written to the server log and are not written to the job log.

## Partitioned steps

Partitioned steps have more subdirectories for each partition. The log files in the *execution ID* directory contain entries from the thread that is running the top-level job. The job logs for the partitions are stored with the following structure:

```
log directory/joblogs/job name/date/instance.job instance ID/execution.execution ID/name of
partitioned step/partition number
```

**Important:** A directory is created in the *name of partitioned step* directory for each partition.

## Split flows

If a split flow occurs in the job, more subdirectories are created to capture the output from the thread of each flow. The log files that are located directly under the *execution ID* directory contains entries from the thread that is running the top-level job. The job logs for individual flow threads are stored with the following structure:

```
log directory/joblogs/job name/date/instance.job instance ID/execution.execution ID/split
ID/flow ID
```

**Important:** A directory is created in the *split ID* directory for each flow.

## Job log events

| If batch job events are enabled, then job log events are published when a job log part is completed and  
| when a job goes to an ended state, such as stopped, failed, or completed. The job log event messages  
| contain multiple JSON properties to help with identifying the message along with the actual job log file  
| content.

| **Important:** The JSON properties are part of the JMS message body and can be retrieved by converting  
| the body text to a `JsonObject` and pulling the specific JSON property from that object.

| The following example illustrates how to retrieve the job log content property.

```
| //The retrieved job log event message  
| Message msg  
| //Convert the Message to a TextMessage
```

```
| TextMessage txtMsg = (TextMessage) msg;
| //Convert the text in the message to a JsonObject
| JsonObject jobLogEventObject = Json.createReader(new StringReader(txtMsg.getText())).readObject();
| //Pull the job log text content from the JsonObject as an example
| JSONArray logContentArray = jobLogEventObject.getJSONArray("contents");
```

| For more information about enabling batch job events, see *Enabling batch job events publishing*.

---

## Liberty: Shared libraries

**8.5.5.0**

Shared libraries are files used by multiple applications. **8.5.5.0** You can use shared libraries and global libraries to reduce the number of duplicate library files on your system.

### Library elements

Liberty libraries have three elements; <folder>, <file>, and <fileset>. For example:

```
<library>
  <folder dir="..." />
  <file name="..." />
  <fileset dir="..." includes="*.jar" scanInterval="5s" />
</library>
```

A specified file must be a container for the resource (for example a JAR file) rather than the resource itself.

If an element in the list is a file, the contents of that JAR or compressed .zip file are searched. If a folder is specified then resources are loaded from that directory.

### Global libraries

Global libraries can be used by any application. JAR files are placed in a global library directory, and then are specified in the class loader configuration for each application.

You can place global libraries in two locations:

- \${shared.config.dir}/lib/global
- \${server.config.dir}/lib/global

If there are files present in these locations at the time an application is started, and that application does not have a <classloader> element configured, the application uses these libraries. If a class loader configuration is present, these libraries are not used unless the global library is explicitly referenced.

For more information, see “Providing global libraries for all Java EE applications” on page 1598.

### Resource files

Within Liberty libraries, you can have resource files defined in the library element. For example,

```
<library>
  <folder dir="..." />
  <file name="..." />
  <fileset dir="..." includes="*.jar" scanInterval="5s" />
  <folder dir="${server.config.dir}/mylibs" />
  <file name="${server.config.dir}/otherlibs/my.jar" />
</library>
```

The folder setting in the previous example, allows all files under the `mylibs` directory to be available on the classpath. You can use this style of entry to have your `.xml` and `.properties` available.

## Library elements

Liberty libraries have three child elements, `<folder>`, `<file>` and `<fileset>`. For example,

```
<library>
  <folder dir="..." />
  <file name="..." />
  <fileset dir="..." includes="*.jar" scanInterval="5s" />
</library>
```

- `<folder>`: All resources under each configured folder will be loadable
- `<file>`: Each configured file should be either a native library or a container for resources (such as a JAR or a ZIP file). All resources within a container are loadable and any other filetype that is specified will have no effect.
- `<fileset>`: Each configured fileset is effectively a collection of files. Each file in the fileset should be a native library or a container for resources (such as a JAR or a ZIP file). All resources within a container are loadable and any other filetype that is specified will have no effect.

For example,

```
<library id="someLibrary">
  <!-- Location of XML and .properties files in the file system for easy editing -->
  <folder dir="${server.config.dir}/editableConfig" />

  <!-- Location of some classes and resources in the file system -->
  <folder dir="${server.config.dir}/extraStuff" />

  <!-- A zip file containing some resources -->
  <file name="${server.config.dir}/lib/someResources.zip" />

  <!-- All the jar files in ther servers lib folder -->
  <fileset dir="${server.config.dir}/lib" includes="*.jar" scanInterval="5s" />
</library>

<application location ="webStore.war">
  <classloader commonLibraryRef="someLibrary" />
</application>
```

The configuration snippet in the previous example, allows all resources under the `editableConfig` directory to be loaded by the `webStore` application.

---

## Loose applications

8.5.5.4

Loose applications are applications that are composed from multiple physical locations, which are provided to the run time via an XML file. Loose applications are supported for Java EE and OSGi applications and are particularly beneficial in a development environment.

### Normal application

Normally an application is contained under one directory (or in one archive), with its content, modules, resources, classdata, and metadata at known locations within that directory. For example: the location of resources for a web application is as follows:

- Library Java archive (JAR) files are stored in `WEB-INF/lib`
- Classes are either in library JAR files or in `WEB-INF/classes`
- The deployment descriptor is in `WEB-INF/web.xml`

- Content to be served is located from the root of the directory

## Loose application

A loose application is described as “a virtual directory that represents the application, where information might be in any location”. It enables development tools, such as WebSphere Application Server Developer Tools, to run applications where the associated files are loaded directly from the workspace, rather than being exported. Examples of associated files are Java classes, JavaServer Pages, or images. If you load the associated files directly from the workspace, it results in a faster build-run-debugging cycle. The content is not present under one directory, but can come from other locations. These locations are specified in an XML configuration file.

There are two ways you can provide the XML file to the run time:

1. By placing the XML file in the `location` attribute in an application configuration element with an appended `.xml` suffix
2. By placing the XML file directly into the `dropins` folder

For example, if you specify `<application location="myapp.war" />`, the run time looks for a file called `myapp.war.xml`. The search rules are the same as for an application directory or archive. If the application files and the `.xml` loose application configuration files are both found, then the loose application configuration file is ignored. For example, if you have `myapp.war` and `myapp.war.xml`, the Liberty server uses `myapp.war` to run the application. You can also deploy loose applications directly into the `dropins` folder. To use the `dropins` folder, follow the naming conventions that are defined for the folder and append `.xml` to the end of the file name.

## Loose application configuration file

The Liberty server uses the loose application configuration file to obtain the application content, rather than locating it from a root directory or single archive. Using the appropriate XML, you can take the following actions:

- Map any physical directory to any location within the application
- Map any physical file to any location within the application
- Map any physical JAR file or directory to any location as a nested archive
- Map multiple physical sources to a single target location (merging)

For example:

1. Map the root of the archive to one location on disk, such as a folder in an Eclipse project.
2. Map a Java `bin/output` folder that is not in the “usual” location into the `WEB-INF/classes` folder. This location might be in a different folder due to your workspace preferences, corporate guidelines, source control project layout guidelines, and so on. You might have multiple Java source and output locations in the same project, and want to map them both to `WEB-INF/classes`.
3. Map an “external” JAR file into the application. This “external” JAR file might be one of the following:
  - A separate Java project that you want to treat like a JAR file in `WEB-INF/lib`
  - A utility JAR file somewhere else on your hard disk drive that you built the `.war` file against, and need to include in `WEB-INF/lib` at run time

## Loose application configuration file examples

You can configure three different elements in the loose application configuration file:

- `<archive>` for archives
- `<file>` for files
- `<dir>` for directories

## Archives

The `<archive>` element is always used as the root of the loose application configuration file. It is also the root of the virtual file system that is represented in the XML. You can nest any of the three elements under the root `<archive>` element. The root `<archive>` element does not have any attributes.

Archive elements can be nested recursively. For `<archive>` elements nested under the root `<archive>` element, you can set the `targetInArchive` attribute. The `targetInArchive` attribute defines the path where the archive appears within the loose defined enclosing archive. You cannot map an archive on the file system as an archive in the application with an `<archive>` element. To use loose application configuration to map an archive on disk, use a `<file>` element instead.

**Note:** The `targetInArchive` attribute value is an absolute path with a leading forward slash (/).

The following code is an example of the root `<archive>` element with another `<archive>` element nested under it:

```
<archive>
  <archive targetInArchive="/jarName.jar">
    <!-- more objects can be embedded here-->
  </archive>
</archive>
```

**Files** You can use the `<file>` element to map a file on your hard disk to a file in your loose application configuration. You can set the following attributes on the `<file>` element:

- `targetInArchive` defines the path where the archive appears within the loose defined enclosing archive.
- `sourceOnDisk` defines the actual location of your file on your file system.

**Note:** The `sourceOnDisk` attribute value is an absolute location. You can use Liberty variables such as `${was.server.dir}`, which are resolved correctly.

The following code is an example of a file in `C:/devFolder/myApplication.zip` that is represented as `/apps/webApplication.war` by the loose application configuration:

```
<file targetInArchive="/apps/webApplication.war"
      sourceOnDisk="C:/devFolder/myApplication.zip" />
```

The following code is an example of an enclosing archive that defines an archive at path `/apps/webApplication.war`. Within the archive, `webApplication.war` defines a file, `jarName.jar` at path `/applications/myApplications`. The actual file location is `c:\devFolder\myApplication.zip`:

```
<archive targetInArchive="/apps/webApplication.war">
  <file targetInArchive="/applications/myApplications/jarName.jar"
        sourceOnDisk="C:/devFolder/myApplication.zip" />
</archive>
```

## Directories

You can use the `<dir>` element to map a directory, and all of its contents on disk, to a directory location in the loose application configuration. The element has the same attributes as the `<file>` element and you use it in a similar way.

The following code is an example of a directory that the loose application configuration shows as being in `/META-INF` and on your file system in `${was.server.dir}/applicationData/myApplication`:

```
<dir targetInArchive="/META-INF"
     sourceOnDisk="${was.server.dir}/applicationData/myApplication" />
```

To add the directory to an archive so it appears to be in `/apps/jarName.jar/META-INF`, embed the `<dir>` element as follows:

```

<archive targetInArchive="/apps/jarName.jar">
  <dir targetInArchive="/META-INF"
        sourceOnDisk="${was.server.dir}/applicationData/myApplication" />
</archive>

```

In both of the previous examples, all files that are in `${was.server.dir}/applicationData/myApplication` are mapped and visible in the loose application configuration under the directory that is mapped by the `targetInArchive` attribute.

## Virtual paths and file names

If you add `<file>` or `<dir>` elements to an archive, the name of the file or directory in the loose archive does not need to be the same as the actual name on disk.

The following code is an example of how you can configure `${was.server.dir}/applicationFiles/newfile.txt` to appear in the archive as `/application.txt`:

```

<archive>
  <file targetInArchive="/application.txt"
        sourceOnDisk="${was.server.dir}/applicationFiles/newfile.txt"/>
</archive>

```

The same concept also holds true for the path of any added file or directory. The physical resource on disk does not need to be in a directory hierarchy that corresponds to the one being declared.

The following code is an example of how you can make `${was.server.dir}/applicationFiles/newfile.txt` appear in the archive as `/only/available/in/application.txt`:

```

<archive>
  <file targetInArchive="/only/available/in/application.txt"
        sourceOnDisk="`${was.server.dir}/applicationFiles/newfile.txt"/>
</archive>

```

In each case, the Liberty server sees the resource by the name and path declared by the `targetInArchive` attribute. The Liberty server can navigate the directory hierarchy declared, even if the hierarchy contains only virtual elements, as in the previous example.

```

<archive>
  <file targetInArchive="/only/available/in/red.txt"
        sourceOnDisk="${was.server.dir}/applicationFiles/newfile.txt" />
<archive targetInArchive="/apps/jarName.jar">
  <dir targetInArchive="/META-INF"
        sourceOnDisk="${was.server.dir}/applicationData/myApplication" />
</archive>

```

## Folders and files with the same name

If you have two folders with the same name in the same virtual location in the loose application configuration, the folders are merged, and the contents of both folders are available. If you have two files with the same target location in the loose archive, the first occurrence of the file is used. The first occurrence is based on a top-down approach to reading the elements of the loose application configuration file.

If the first file found is the wrong file, reorder the XML so that the element that contains the version of the file you want is processed first. The first occurrence applies to files defined in `<dir>` elements and files that are defined in `<file>` elements. The first occurrence of a file with the same name and virtual location is the one returned from the virtual file system.

## Considerations for loose applications

For all loose configured applications, the files are not on disk in the hierarchy that they are declared to be. If your applications directly access their own resources, and expect them to be arranged on disk as they would be with an expanded war or ear layout, they might exhibit unexpected behavior.

You can use `ServletContext.getRealPath` in your applications to discover physical resource paths. `ServletContext.getRealPath` can discover file paths to open to read or write data, and obtain directories. However, if you use `ServletContext.getRealPath` in web applications to obtain a path for `"/"`, you cannot use this path to navigate the application on disk.

`ServletContext.getRealPath` allows only a single physical path to be returned, and the loose application might have merged multiple directories to form one path visible to the application.

Consider the following configuration:

```
<archive>
  <dir targetInArchive="/"
        sourceOnDisk="c:\myapplication" />
  <dir targetInArchive="/web/pages"
        sourceOnDisk="c:\webpagesforapplication" />
</archive>
```

An application that directly accesses `/web/pages` and then navigates up the directory hierarchy, finds that the parent of the physical path of `/web/pages` is `c:\` and not `/web`. `c:\` has no `pages` directory and no parent directory.

These considerations apply only if your applications attempt to directly access the content on disk, and perform their own path navigation based on an assumption of a corresponding hierarchical layout on disk. The same applications also encounter issues if they are deployed as an archive. These applications generally experience issues with portability.

## Complex example

The following code is a more complex example of loose application configuration. This example uses all of the elements and creates a complex mapping of files and directories:

```
<archive>
  <dir targetInArchive="/appResources"
        sourceOnDisk="{was.server.dir}/applicationFiles" />
  <archive targetInArchive="application.jar">
    <dir targetInArchive="/src"
          sourceOnDisk="{was.server.dir}/applicationCode/src" />
  </archive>
  <archive targetInArchive="webApp.war">
    <dir targetInArchive="/META-INF"
          sourceOnDisk="{was.server.dir}/manifestFiles/" />
    <dir targetInArchive="/WEB-INF"
          sourceOnDisk="c:/myWorkspace/webAppProject/web-inf" />
    <archive targetInArchive="/WEB-INF/lib/myUtility.jar">
      <dir targetInArchive="/"
            sourceOnDisk="c:/myWorkspace/myUtilityProject/src" />
      <file targetInArchive="/someJar.jar"
            sourceOnDisk="c:/myWorkspace/myUtilityProject/aJar.jar" />
    </archive>
  </archive>
  <file targetInArchive="/myjar.jar"
        sourceOnDisk="{was.server.dir}/apps/application.zip" />
</archive>
```

---

## Discovering REST API documentation on a Liberty server

8.5.5.8

You can discover your REST API documentation. Use the API Discovery feature to find what REST APIs are available on a Liberty server and then use the Swagger user interface to invoke the found REST endpoints.

### Procedure

1. Add the `apiDiscovery-1.0` feature to a feature manager in the `server.xml` file of the Liberty server whose available REST APIs you want to find.

The `apiDiscovery-1.0` feature enables the REST API discovery bundles in the product. The feature also exposes documentation from Liberty REST endpoints such as JMX, if the server configuration uses the `restConnector-1.0` feature, and collectives, if the server configuration uses the `collectiveController-1.0` feature.

**8.5.5.9** The `apiDiscovery-1.0` feature enabled on a Liberty collective controller server finds the REST APIs available on the controller and on its member servers with the `apiDiscovery-1.0` feature enabled.

Ensure the server configuration has all features needed for your deployed application, such as `servlet-3.0`, `jsp-2.2`, and so on. Also ensure the ports and user registry settings are correct for the deployed application.

The following `server.xml` file has the `apiDiscovery-1.0` feature:

```
<server>
  <featureManager>
    <feature>apiDiscovery-1.0</feature>
  </featureManager>

  <httpEndpoint id="defaultHttpEndpoint"
    host="*"
    httpPort="8010"
    httpsPort="8020"/>

  <keyStore id="defaultKeyStore" password="Liberty"/>

  <basicRegistry id="basic" realm="ibm/api">
    <user name="bob" password="bobpwd" />
  </basicRegistry>
</server>
```

2. Expose the Swagger 2.0 documentation in Liberty REST endpoints.

You can configure the location of your API documentation in either of two ways:

- Use the `getDocument` method of the SPI `com.ibm.wsspi.rest.api.discovery.APIProvider` interface.

The `getDocument` method enables OSGi bundles from extension features to contribute REST API documents to the overall “master” documentation. For this release, the only supported `DocType` are `DocType.Swagger_20_JSON` and `DocType.Swagger_20_YAML`. Implementers of this interface can return the serialized JSON or YAML document as a `java.lang.String` value, or they can pass in a file reference (prefixed with `file:///`) to the JSON or YAML file location.

- Use a deployed web application.

Each web module can contribute its own REST API document. Multiple WAR files inside an enterprise application (EAR) file can have different Swagger 2.0 documents.

The easiest way to expose the documentation of web modules is to include a `swagger.json` or `swagger.yaml` file inside the corresponding `META-INF` folder. During application deployment, the API Discovery feature looks for a `META-INF/swagger.json` value for each of the web modules. If a `META-INF/swagger.json` value is not found then the API Discovery feature looks for a `META-INF/swagger.yaml` value.

Another way to expose the REST API documentation for a web module is in a `server.xml` configuration file. Put a `webModuleDoc` element for each web module in a parent `apiDiscovery` element; for example:

```
<apiDiscovery>
  <webModuleDoc contextRoot="/30ExampleServletInEar" enabled="true" docURL="/swagger.json" />
  <webModuleDoc contextRoot="/22ExampleServlet" enabled="false" />
  <webModuleDoc contextRoot="/custom" enabled="true" docURL="http://petstore.swagger.io/v2/swagger.json" />
</apiDiscovery>
```

The `webModuleDoc` element must have a `contextRoot` attribute to uniquely identify the web module whose documentation you want to expose.

An optional attribute, `enabled`, toggles the API discovery for a web module. The default of this attribute is `true`.

The `docURL` attribute specifies where to find the documentation for the web module. The `docURL` value can start with a forward slash (`/`) so that the URL is relative to the context root; for example, `/30ExampleServletInEar/swagger.json`. Or the `docURL` value can start with `http` or `https` for an absolute URL that identifies the complete location of the documentation.

**8.5.5.9** If the web application does not provide a `swagger.json` or `swagger.yaml` file and the application contains JAX-RS annotated resources, you can automatically generate the Swagger document. The server configuration must have the `apiDiscovery-1.0` feature and the `jaxrs-1.1` or `jaxrs-2.0` feature; for example:

```
<featureManager>
  <feature>apiDiscovery-1.0</feature>
  <feature>jaxrs-1.0</feature>
</featureManager>
```

The product scans all classes in the web application for JAX-RS and Swagger annotations, searching for classes with `@Path`, `@Api`, and `@SwaggerDefinition` annotations. The product also automatically generates a corresponding Swagger document during the web application deployment or startup.

**8.5.5.9** You can also use the `apiDiscovery-1.0` feature to merge previously generated documentation with the documentation that it finds during annotation scanning. The product searches for a `META-INF/stub/swagger.json` or `META-INF/stub/swagger.yaml` file in the web module. If the feature finds either of these files, the feature generates a Swagger document that contains both the content of the file and any JAX-RS and Swagger annotations that are in the web module. You can use this feature to document non-JAX-RS servlets because the documentation is automatically merged with the JAX-RS portions.

**8.5.5.9** Another way to expose the REST API documentation for a web module is to add `swagger.json` or `swagger.yaml` to the context root of the web application; for example:

```
http://host:http_port/context_root/swagger.json
```

or

```
http://host:http_port/context_root/swagger.yaml
```

A call to `context_root/swagger.json` or `context_root/swagger.yaml` returns the documentation for the context root in the requested JSON or YAML format. During web module startup, the API Discovery feature pulls any available `context_root/swagger.json` into the aggregated document from `/ibm/api/docs` and `/ibm/api/explorer`. If `context_root/swagger.json` is not available, then the API Discovery feature pulls any available `context_root/swagger.yaml` into the aggregated document from `/ibm/api/docs` and `/ibm/api/explorer`. The `apiDiscovery-1.0` feature can handle `swagger.json` or `swagger.yaml` virtually, which means that if the web application has a `server.xml` file that configures a `docURL` attribute, a `swagger.json` or `swagger.yaml` file in the `META-INF` folder, or JAX-RS and Swagger annotations, then the call to `context_root/swagger.json` or `context_root/swagger.yaml` returns the documentation for this other configuration in the requested JSON or YAML format.

### 3. Discover your API documentation.

After you configure the location of your API documentation, you can discover it in the following ways:

- Use the GET `https://host:https_port/ibm/api/docs` endpoint.  
This endpoint provides a valid Swagger 2.0 document with all available Liberty REST APIs merged into a single document. This is useful for consumer applications that want to programmatically navigate the set of available APIs, such as an API Management solution. Including an optional Accept header with an `application/yaml` value provides the Swagger 2.0 document in YAML format. This endpoint has a multiple-cardinality, optional query parameter called `root` that can filter the found context roots. For example, a call to GET `https://host:https_port/ibm/api/docs?root=/myApp` retrieves a Swagger 2.0 document that only has the documentation for the `myApp` context root.

- Use the GET `https://host:https_port/ibm/api/explorer` endpoint.  
This endpoint provides an attractive, rendered HTML page that displays the content from the `/ibm/api/docs` URL. This page follows the same pattern as the standard online sample (<http://petstore.swagger.io/>), so that users can invoke the REST API. This endpoint helps you explore the available REST APIs on a Liberty server, and perhaps invoke them from the page. A filter input box enables a comma-separated list of context roots to filter the content. This filtering works like the `root` query parameter. You can test drive the APIs by providing the required input values and click the "Try it out" button.

- **8.5.5.9** If a collective controller, use the GET `https://host:https_port/ibm/api/collective/docs` endpoint.

This endpoint on the collective controller provides a valid Swagger 2.0 document with REST APIs available from the collective controller and its members with the `apiDiscovery-1.0` feature enabled merged into a single document. This is useful for consumer applications that want to programmatically navigate the set of available APIs, such as an API Management solution. Including an optional Accept header with an `application/yaml` value provides the Swagger 2.0 document in YAML format. This endpoint has two multiple-cardinality, optional query parameters called `root` and `serverID`.

Query parameter `root` can filter the found context roots. For example, a call to GET `https://host:https_port/ibm/api/collective/docs?root=/myApp` retrieves a Swagger 2.0 document that only has the documentation for the `myApp` context root.

Query parameter `serverID` can filter the REST APIs available from a Liberty server. The format of `serverID` is `hostName,userDir,serverName`. The format provides the name of the host followed by a comma (,) followed by the installation directory followed by a comma (,) followed by the name of the server. For example, a call to GET `https://host:https_port/ibm/api/collective/docs?serverID=samplehost.com:8020,/users/admin/wlp/usr,server1` retrieves a Swagger 2.0 document that only has the documentation for REST APIs available from the Liberty server with the specified `serverID`.

- **8.5.5.9** If a collective controller, use the GET `https://host:https_port/ibm/api/collective/explorer` endpoint.

This endpoint on the collective controller provides an attractive, rendered HTML page that displays the content from the `/ibm/api/collective/docs` URL. This endpoint helps you explore the available REST APIs on the entire collective, and perhaps invoke them from the page. A filter input box at a top corner of the page enables a comma-separated list of context roots and server ID to filter the content. The format of the server ID is `"hostName,userDir,serverName"`. Quotation marks (") must surround the server ID. If you would like to test drive the APIs using the "Try it out" button, you will need to setup Cross Origin Request Sharing (CORS) in the `server.xml` of the member server.

For example, the following snippet is required in the `server.xml` of the member server which provide the API `/IBMJMXConnectorREST/mbeanCount`.

```
<cors domain="/IBMJMXConnectorREST/mbeanCount"
      allowedOrigins="https://<controller_hostname>:<https_port>"
      allowedMethods="GET,POST,DELETE,PUT,PATCH,OPTIONS"
      allowedHeaders="Content-Type,api_key,Authorization"
      allowCredentials="true"
/>
```

For further information on setting up CORS, see [Configuring Cross Origin Request Sharing on a Liberty server](#).

**Note:** The CORS requirement is only applicable to the collective version of the Swagger UI ([https://host:https\\_port/ibm/api/collective/explorer](https://host:https_port/ibm/api/collective/explorer)).

**8.5.5.9** After you enable the `apiDiscovery-1.0` feature, the management bean (MBean) that has the `ObjectName` value `WebSphere:feature=apiDiscovery,name=APIDiscovery` is registered in the Liberty MBeanServer. This MBean provides the following attributes:

- The `DocumentationURL` attribute is the full URL of the `/ibm/api/docs` endpoint, and it displays the raw JSON or YAML documentation.
- The `ExplorerURL` attribute is the full URL of the `/ibm/api/explorer` endpoint, and it displays the rendered UI of the documentation.

You can use this MBean to learn whether REST API Discovery is enabled and where a client can reach it.

## Subscribe to Liberty REST API updates

**8.5.5.9**

The Liberty REST API discovery feature now exposes a new REST API, `/ibm/api/docs/subscription`, which allows users to subscribe to any REST API update, such as new APIs being available or old APIs being removed. This is useful when a user wants to be notified immediately of any changes in the endpoints that are provided by a particular Liberty instance.

- Enable subscriptions
- Example request and response

### Enable subscriptions

In addition to the base `apiDiscovery-1.0` configuration, it is required to also configure either `websocket-1.0` or `websocket-1.1` in your `server.xml`.

```
<server>
  <featureManager>
    <feature>apiDiscovery-1.0</feature>
    <feature>websocket-1.1</feature>
  </featureManager>

  <httpEndpoint id="defaultHttpEndpoint"
    host="*"
    httpPort="8010"
    httpsPort="8020"/>

  <keyStore id="defaultKeyStore" password="Liberty"/>

  <basicRegistry id="basic" realm="ibm/api">
    <user name="bob" password="bobpwd" />
  </basicRegistry>
</server>
```

The `/ibm/api/docs/subscription` endpoint allows for POST requests with a JSON payload in the format:

```
{ "docType" : String }
```

Where the `String` can be one of `Swagger_20_JSON` or `Swagger_20_YAML`. The returning JSON payload outlines the type of subscription feed and its URL.

### Example request and corresponding response

Request:

```
{"docType":"Swagger_20_JSON"}
```

Response:

```
{
  "feedType": "websocket",
  "feedURL": "wss://myserver.com:8020/ibm/api/docs/subscription/websocket/60db0d79-1863-48f5-a0f9-4fe22a27b82d"
}
```

You can now use a websocket client to connect to the feed URL. Once connected, any further updates to REST APIs in the Liberty server is pushed through the websocket. The update is either in JSON or YAML format, depending on the subscription.

## Subscribing to Liberty REST API updates in a collective

8.5.5.9

Use the subscription API in the collective controller to immediately learn about new REST APIs, removed APIs, or changes to APIs such as changes in the endpoints from a specific collective member server.

### Before you begin

The `/ibm/api/collective/docs/subscription` API is in the Liberty REST API discovery feature. To subscribe to updates to REST APIs from collective member servers, you must first complete the procedure in "Discovering REST API documentation on a Liberty server" on page 2260 for a collective controller.

### Procedure

#### 1. Enable subscriptions.

Add the `websocket-1.0` or `websocket-1.1` feature to the collective controller `server.xml` file; for example:

```
<server>
  <featureManager>
    <feature>collectiveController-1.0</feature>
    <feature>apiDiscovery-1.0</feature>
    <feature>websocket-1.1</feature>
  </featureManager>

  <!-- some collective controller configurations are omitted -->

  <httpEndpoint id="defaultHttpEndpoint"
    host="*"
    httpPort="8010"
    httpsPort="8020"/>

  <keyStore id="defaultKeyStore" password="Liberty"/>

  <basicRegistry id="basic" realm="ibm/api">
    <user name="bob" password="bobpwd" />
  </basicRegistry>
</server>
```

The `/ibm/api/collective/docs/subscription` endpoint enables POST requests with a JSON payload in the following format:

```
{ "docType" : String }
```

*String* is either `Swagger_20_JSON` or `Swagger_20_YAML`. The returning JSON payload outlines the type of subscription feed and its URL.

For example, the following request:

```
{"docType": "Swagger_20_JSON"}
```

returns a response such as:

```
{
  "feedType": "websocket",
  "feedURL": "wss://myserver.com:8020/ibm/api/collective/docs/subscription/websocket/60db0d79-1863-48f5-a0f9-4fe22a27b82d"
}
```

#### 2. Use a websocket client to connect to the feed URL.

You can write code or use a third-party websocket client to connect to the feed URL. Once connected, any further updates to REST APIs in the Liberty server are pushed through the websocket. The update is either in JSON or YAML format, depending on the subscription.

## REST endpoints for pushing APIs into IBM API Connect

8.5.5.9

Use the REST endpoint, which is a central location for both on-premises and cloud Liberty users, to visualize, call, and push APIs into IBM API Connect.

### Pushing deployed REST endpoints into IBM API Connect

To push deployed REST endpoints into IBM API Connect, you must call a new REST endpoint, `/ibm/api/docs/apiconnect`, which is exposed by the `apiDiscovery-1.0` feature in the server configuration. Administrators and developers can use the REST endpoints to expose assets from a Liberty instance to any enterprise developer who is searching the IBM API Connect framework catalogs.

### Providing a product definition

All APIs are referenced by a product and exposed from a catalog. Therefore, the caller provides a product definition that Liberty uses to refer to its RESTful APIs and push the resulting product into IBM API Connect. A sample product is provided in this topic.

### Exposing assets of a Liberty collective into IBM API Connect

Using a corresponding Liberty collective endpoint, `/ibm/api/collective/docs/apiconnect`, you can expose all assets of a Liberty Collective into IBM API Connect with a single RESTful trigger. The Liberty collective endpoint can expose thousands of APIs to any cloud developer connected to API Connect. See the Liberty RESTful API registry, `/ibm/api/explorer`, for the full Swagger definition of this endpoint.

### Endpoint summary

HTTP Request method: POST

URL: `https://server:https_port/ibm/api/docs/apiconnect`

### Required headers

#### X-APIM-Authorization

Credentials to connect to API Connect display in the two following forms:

- username and password
- xyz where xyz is the base64 encoded version of username: password.

### Required query parameters

**Server** The name of the IBM API Connect server, starting with `https://`.

#### Catalog

The name of the catalog that hosts the resulting product.

#### Organization

The name of the organization of the caller.

### Optional query parameters

#### apiRoot

A multi-cardinality parameter that specifies exactly which context roots, such as, `apiRoot=/myApp`,

the caller wants to push into API Connect. By default, Liberty includes any deployed application except known Liberty runtime Web Application Bundles. This parameter is useful when you want to filter which applications get exposed.

#### **member ID (only available for the Collective variant)**

A multi-cardinality parameter that specifies the ID of the exact Collective Members from which the caller wants to expose assets. This ID is composed of a string with the host name, the URLEncoded user dir, and the server name, all separated by a comma, for example: myHost.com,%2Ftmp%2Fwlp%2Fusr, server1.

#### **Input body**

Product definition in either in YAML or JSON code. See the following YAML example:

```
product: "1.0.0"
  info:
    name: "pushed-product"
    title: "A Product that encapsulates Liberty APIs"
    version: "1.0.0"
  visibility:
    view:
      enabled: true
      type: "public"
      tags:
        - "string"
      orgs:
        - "string"
    subscribe:
      enabled: true
      type: "authenticated"
      tags:
        - "string"
      orgs:
        - "string"
  apis:
    liberty:
      name: "liberty-api:1.0.0"
      x-ibm-configuration:
        phase: "realized"
        testable: true
        enforced: true
        cors:
          enabled: true
        assembly:
          execute:
            -
              invoke:
                target-url: "${gateway.target}"
                title: "Invocation"
                description: "Invoking back-end service"
  plans:
    default:
      title: "Default Plan"
      rate-limit:
        hard-limit: false
        value: "100/hour"
      approval: false
  createdAt: "2016-04-18T20:33:22.937Z"
  createdBy: "string"
```

---

## Chapter 11. Monitoring the Liberty server runtime environment

You can use the `monitor-1.0` feature to monitor the server runtime environment.

### About this task

To enable monitoring for your Liberty server, you add `monitor-1.0` Liberty feature in the `server.xml` file.

The `monitor-1.0` feature provides monitoring support for user runtime components.

- JVM
- Web applications
- Thread pool
- **8.5.5.0** JAX-WS endpoints
- **8.5.5.0** Session management
- **8.5.5.0** ConnectionPool

For more details, see “Liberty features” on page 826.

### Procedure

1. Add the `monitor-1.0` feature and the monitoring starts.

**Note:** **8.5.5.3** If you launch the server by not using the server script (`server.sh` or `server.bat`) on a Java Virtual Machine (JVM), ensure that the JavaAgent is configured for JVM as given in the following example: `agentlib=-javaagent:<path to liberty install>/bin/tools/ws-javaagent.jar`.

2. Monitoring data is reported as standard MBeans.
3. You can use JConsole to connect to JVM and look at the performance data by clicking each attribute of the MBean.

The MBeans for monitoring are as following:

- `WebSphere:type=JvmStats`
  - `WebSphere:type=ServletStats,name=*`
  - `WebSphere:type=ThreadPoolStats,name=Default Executor`
  - **8.5.5.0** `org.apache.cxf:type=WebServiceStats,service=*,port=*`
  - **8.5.5.0** `WebSphere:type=SessionStats,name=*`
  - **8.5.5.0** `WebSphere:type=ConnectionPool,name=*`
4. Optional: The same data is available with traditional PMI MBean (Perf MBean). Note that the Perf MBean is stabilized.

---

### Liberty:JVM monitoring

You can use the `JvmStats` MBean for JVM monitoring in Liberty.

Each Liberty instance has one `JvmStats` MBean.

The `ObjectName` for identifying JVM MBean is:

```
WebSphere:type=JvmStats
```

Available Instances = 1

This MBean is responsible for reporting performance of JVM. Following attributes are available for JVM.

#### Heap Information

- Amount of free heap available (in Bytes)
- Total used memory by JVM for from heap (in Bytes)
- Heap size (in Bytes)

#### CPU Information

- Percentage of CPU consumed by this JVM

#### Garbage Collection (GC) Information

- Number of times that GC happened since JVM started
- Total time taken by GC activity

#### General Information

- Time in milliseconds since JVM has started.

#### Counter definitions (Attributes to MBean)

- Heap: Heap size used for current JVM.
- FreeMemory: Free heap available for current JVM.
- UsedMemory: Used heap for current JVM.
- ProcessCPU: Percentage of CPU used by JVM process.
- GcCount: Number of times GC has happened since JVM starts.
- GcTime: Total accumulated value of GC time.
- UpTime: Time in milliseconds, since JVM has started.

#### 8.5.0.1 Management Interface

The management interface of JVM monitoring is `com.ibm.websphere.monitor.jmx.JvmMBean`.

**8.5.0.1** You can use the management interface to obtain a proxy object. See “Liberty:Examples of accessing MBean attributes and operations” on page 1654.

For more information about the management interface, see the Java API document for Liberty. The Java API documentation for each Liberty API is available in a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

---

## Liberty:Web application monitoring

You can use a servlet MBean for web application monitoring of Liberty.

Performance data is available for each Servlet in the Web Application. Each servlet has its own MBean.

The ObjectName for identifying each servlet MBean is:

```
WebSphere:type=ServletStats,name=<AppName>.<ServletName>
```

For example:

```
WebSphere:type=ServletStats,name=snoop.Alpine Snoop Servlet
WebSphere:type=ServletStats,name=MyApp.MyServlet
```

This MBean is responsible for reporting ServletStats for each servlet. Following key data is available for ServletStats MBean:

- Request Count
- Response Time
- Servlet Name
- Application Name

#### Counter definitions (Attributes to MBean)

- `AppName`: Name of the application.
- `ServletName`: Name of the servlet.
- `RequestCount`: Number of hits to this servlet.
- `ResponseTime`: Average response time (nano-seconds).
- `Description`: Description of counter.
- `RequestCountDetails`: RequestCount details including last time stamp.
- `ResponseTimeDetails`: ResponseTime details including number of snapshot taken, min, and max values.

#### 8.5.0.1 Management Interface

The management interface of web application monitoring is

`com.ibm.websphere.webcontainer.ServletStatsMBean`. 8.5.0.1 You can use the management interface to obtain a proxy object. See “Liberty:Examples of accessing MBean attributes and operations” on page 1654.

For more information about the management interface, see the Java API document for Liberty. The Java API documentation for each Liberty API is available in a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

---

## Liberty:ThreadPool monitoring

You can use a ThreadPool MBean for thread pool monitoring in Liberty.

All Web Requests executes in the thread pool, named **Default Executor** thread pool. You can monitor the usage of **Default Executor** thread pool using ThreadPoolMBean.

The ObjectName for identifying MBean for thread pool is :

```
WebSphere:type=ThreadPoolStats,name=Default Executor
```

Key Performance data available for ThreadPool are:

- Threads in the pool which represents the pool size.
- Active threads which are serving requests.

#### Attributes for ThreadPool

- `ActiveThreads`
- `PoolSize`
- `PoolName` (Only supports Default Executor thread pool)

### 8.5.0.1 Management Interface

The management interface of ThreadPool monitoring is

`com.ibm.websphere.monitor.jmx.ThreadPoolMBean`. **8.5.0.1** You can use the management interface to obtain a proxy object. See “Liberty:Examples of accessing MBean attributes and operations” on page 1654.

For more information about the management interface, see the Java API document for Liberty. The Java API documentation for each Liberty API is available in a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

---

## Liberty:JAX-WS monitoring

### 8.5.5.0

You can use the endpoint MBean for JAX-WS monitoring of Liberty.

Performance data is available for each endpoint and operation in the JAX-WS application. Each web service endpoint has its own MBean.

The ObjectName for identifying each endpoint MBean might be in one of the following formats:

```
org.apache.cxf:bus.id=<bus.name>,type=Performance.Counter.Server,service="<NameSpace><ServiceName>",port="<PortName>"
org.apache.cxf:bus.id=<bus.name>,type=Performance.Counter.Client,service="<NameSpace><ServiceName>",port="<PortName>"
```

For example:

```
org.apache.cxf:bus.id=JaxWsLibertyDemo-Server-Bus,type=Performance.Counter.Server,
service="{http://jaxws.samples/}SimpleEchoService",port="SimpleEchoPort"
org.apache.cxf:bus.id=JaxWsLibertyDemo-Server-Bus,type=Performance.Counter.Client,
service="{http://jaxws.samples/}SimpleEchoService",port="SimpleEchoPort"
```

This MBean is responsible for reporting the web service status of each endpoint and operation.

#### Counter definitions (Attributes to MBean)

- AvgResponseTime: Average response time (millisecond).
- MaxResponseTime: Maximum response time (millisecond).
- MinResponseTime: Minimum response time (millisecond).
- NumInvocations: Number of invocations to this endpoint or operation.
- NumCheckedApplicationFaults: Number of checked application faults.
- NumLogicalRuntimeFaults: Number of logical runtime faults.
- NumRuntimeFaults: Number of runtime faults.
- NumUncheckedApplicationFaults: Number of unchecked application faults.
- TotalHandlingTime: Total response handling time (millisecond)..

#### Management Interface

The management interface for web service application monitoring is

`org.apache.cxf.management.counters.ResponseTimeCounterMBean`. **8.5.0.1** You can use the management interface to obtain a proxy object. See “Liberty:Examples of accessing MBean attributes and operations” on page 1654.

For more information about the `org.apache.cxf.management.counters.ResponseTimeCounterMBean`, see the Apache CXF Javadoc.

## SIP application monitoring

8.5.5.9

Session Initiation Protocol (SIP) Performance Monitoring Infrastructure (PMI) is a component that collects SIP performance metrics of a running application server. To monitor the SIP metrics, you must enable PMI on your server. To enable monitoring for SIP, add `monitor-1.0` and `sipServlet-1.1` Liberty features to the `server.xml` file.

All Liberty SIP PMI counters are shown by standard MBeans.

The SIP container provides the following MBean interfaces for the SIP counters:

- `WebSphere:type=SipContainerBasicCounters,name=SipContainer.Basic`
- `WebSphere:type=TaskDurationCounters,name=SipContainer.TaskDuration`
- `WebSphere:type=InboundRequestCounters,name=SipContainer.InboundRequest`
- `WebSphere:type=OutboundRequestCounters,name=SipContainer.OutboundRequest`
- `WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse`
- `WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse`
- `WebSphere:type=QueueMonitoringModule,name=SipContainer.QueueMonitor`

Each interface shows a different set of SIP PMI metrics. Refer to the tables for module details. You can view the SIP PMI counters in multiple ways:

- Use JConsole to connect to JVM and look at the SIP PMI counters by clicking each attribute of the MBean.
- Create your own JMX client application to inspect the counters by starting the MBean operations.

For more information about how to create a JMX client to start the MBean operations, see [Connecting to Liberty by using JMX and Liberty: Examples of accessing MBean attributes and operations](#). SIP provides the following counters in PMI to monitor SIP performance.

*Table 177. SIP container basic counters.* The object name of the MBean from which the counters can be retrieved is: `"WebSphere:type=SipContainerBasicCounters,name=SipContainer.Basic"`. To retrieve the attributes, use the `JMXConnection.getAttribute` method. For example:  
`_connection.getAttribute("WebSphere:type=SipContainerBasicCounters,name=SipContainer.Basic", "SipAppSessions")`.

This table lists the SIP container basic counters.

Name	Attribute	Description	Granularity
Incoming traffic	<code>ReceivedSipMsgs</code>	The average number of messages that are handled by the container and calculated over a configurable period	Server
New SIP application sessions	<code>NewSipApplications</code>	The average number of new SIP application sessions created in the container and calculated over a configurable period	Server
Response time	<code>SipRequestProcessing</code>	The average amount of time that it takes between when a message gets into the container and when a response is sent from the container	Server

*Table 177. SIP container basic counters (continued).* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=SipContainerBasicCounters,name=SipContainer.Basic". To retrieve the attributes, use the JMXConnection.getAttribute method. For example: `_connection.getAttribute("WebSphere:type=SipContainerBasicCounters,name=SipContainer.Basic", "SipAppSessions")`.

This table lists the SIP container basic counters.

Name	Attribute	Description	Granularity
Queue size	InvokerSize	The size of the invoke queue in the product	Server
Rejected SIP messages	RejectedMessages	The number of rejected SIP messages	Server
SIP timer invocations	SipTimersInvocations	The number of invocations of the SIP timers (Timer A, Timer B, Timer C, Timer D, Timer E, Timer F, Timer G, Timer H)	Server
Number of active SIP sessions	SipSessions	The number of SIP sessions that belong to each application	Server
Number of active SIP application sessions	SipAppSessions	The number of SIP application sessions that belong to each application	Server

*Table 178. SIP container inbound requests.* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=InboundRequestCounters,name=SipContainer.InboundRequest". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=InboundRequestCounters,name=SipContainer.InboundRequest", "getTotalInboundRequests", _appName, "INVITE")`.

This table lists the inbound request counters.

Name	Method	Description	Granularity
Number of inbound NOT SIP STANDARD requests	<code>getTotalInboundRequests(appName, "NOTSIPSTANDARD");</code>	Number of inbound NOT SIP STANDARD requests that belong to each application	Application
Number of inbound REGISTER requests	<code>getTotalInboundRequests(appName, "REGISTER");</code>	Number of inbound REGISTER requests that belong to each application	Application
Number of inbound INVITE requests	<code>getTotalInboundRequests(appName, "INVITE");</code>	Number of inbound INVITE requests that belong to each application	Application
Number of inbound ACK requests	<code>getTotalInboundRequests(appName, "ACK");</code>	Number of inbound ACK requests that belong to each application	Application
Number of inbound OPTIONS requests	<code>getTotalInboundRequests(appName, "OPTIONS");</code>	Number of inbound OPTIONS requests that belong to each application	Application
Number of inbound BYE requests	<code>getTotalInboundRequests(appName, "BYE");</code>	Number of inbound BYE requests that belong to each application	Application

*Table 178. SIP container inbound requests (continued).* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=InboundRequestCounters,name=SipContainer.InboundRequest". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=InboundRequestCounters,name=SipContainer.InboundRequest", "getTotalInboundRequests", _appName, "INVITE")`.

This table lists the inbound request counters.

Name	Method	Description	Granularity
Number of inbound CANCEL requests	<code>getTotalInboundRequests(applicationName, "CANCEL");</code>	Number of inbound CANCEL requests that belong to each application	Application
Number of inbound PRACK requests	<code>getTotalInboundRequests(applicationName, "PRACK");</code>	Number of inbound PRACK requests that belong to each application	Application
Number of inbound INFO requests	<code>getTotalInboundRequests(applicationName, "INFO");</code>	Number of inbound INFO requests that belong to each application	Application
Number of inbound SUBSCRIBE requests	<code>getTotalInboundRequests(applicationName, "SUBSCRIBE");</code>	Number of inbound SUBSCRIBE requests that belong to each application	Application
Number of inbound NOTIFY requests	<code>getTotalInboundRequests(applicationName, "NOTIFY");</code>	Number of inbound NOTIFY requests that belong to each application	Application
Number of inbound MESSAGE requests	<code>getTotalInboundRequests(applicationName, "MESSAGE");</code>	Number of inbound MESSAGE requests that belong to each application	Application
Number of inbound PUBLISH requests	<code>getTotalInboundRequests(applicationName, "PUBLISH");</code>	Number of inbound PUBLISH requests that belong to each application	Application
Number of inbound REFER requests	<code>getTotalInboundRequests(applicationName, "REFER");</code>	Number of inbound REFER requests that belong to each application	Application
Number of inbound UPDATE requests	<code>getTotalInboundRequests(applicationName, "UPDATE");</code>	Number of inbound UPDATE requests that belong to each application	Application

*Table 179. SIP container inbound responses.* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse", "getTotalInboundResponses", _appName, "100")`.

This table lists the inbound response counters.

Name	Method	Description	Granularity
Number of inbound 100 responses	<code>getTotalInboundResponses(applicationName, "100");</code>	Number of inbound 100 (Trying) responses that belong to each application	Application
Number of inbound 180 responses	<code>getTotalInboundResponses(applicationName, "180");</code>	Number of inbound 180 (Ringing) responses that belong to each application	Application

Table 179. SIP container inbound responses (continued). The object name of the MXBean from which the counters can be retrieved is: "WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse", "getTotalInboundResponses", _appName, "100")`.

This table lists the inbound response counters.

Name	Method	Description	Granularity
Number of inbound 181 responses	<code>getTotalInboundResponses(applicationName, "181");</code>	Number of inbound 181 (Call being forwarded) responses that belong to each application	Application
Number of inbound 182 responses	<code>getTotalInboundResponses(applicationName, "182");</code>	Number of inbound 182 (Call Queued) responses that belong to each application	Application
Number of inbound 183 responses	<code>getTotalInboundResponses(applicationName, "183");</code>	Number of inbound 183 (Session Progress) responses that belong to each application	Application
Number of inbound 200 responses	<code>getTotalInboundResponses(applicationName, "200");</code>	Number of inbound 200 (OK) responses that belong to each application	Application
Number of inbound 202 responses	<code>getTotalInboundResponses(applicationName, "202");</code>	Number of inbound 202 (Accepted) responses that belong to each application	Application
Number of inbound 300 responses	<code>getTotalInboundResponses(applicationName, "300");</code>	Number of inbound 300 (Multiple choices) responses that belong to each application	Application
Number of inbound 301 responses	<code>getTotalInboundResponses(applicationName, "301");</code>	Number of inbound 301 (Moved Permanently) responses that belong to each application	Application
Number of inbound 302 responses	<code>getTotalInboundResponses(applicationName, "302");</code>	Number of inbound 302 (Moved Temporarily) responses that belong to each application	Application
Number of inbound 305 responses	<code>getTotalInboundResponses(applicationName, "305");</code>	Number of inbound 305 (Use Proxy) responses that belong to each application	Application
Number of inbound 380 responses	<code>getTotalInboundResponses(applicationName, "380");</code>	Number of inbound 380 (Alternative Service) responses that belong to each application	Application
Number of inbound 400 responses	<code>getTotalInboundResponses(applicationName, "400");</code>	Number of inbound 400 (Bad Request) responses that belong to each application	Application
Number of inbound 401 responses	<code>getTotalInboundResponses(applicationName, "401");</code>	Number of inbound 401 (Unauthorized) responses that belong to each application	Application

Table 179. SIP container inbound responses (continued). The object name of the MXBean from which the counters can be retrieved is: "WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse", "getTotalInboundResponses", _appName, "100").`

This table lists the inbound response counters.

Name	Method	Description	Granularity
Number of inbound 402 responses	<code>getTotalInboundResponses(applicationName, "402");</code>	Number of inbound 402 (Payment Required) responses that belong to each application	Application
Number of inbound 403 responses	<code>getTotalInboundResponses(applicationName, "403");</code>	Number of inbound 403 (Forbidden) responses that belong to each application	Application
Number of inbound 404 responses	<code>getTotalInboundResponses(applicationName, "404");</code>	Number of inbound 404 (Not Found) responses that belong to each application	Application
Number of inbound 405 responses	<code>getTotalInboundResponses(applicationName, "405");</code>	Number of inbound 405 (Method Not Allowed) responses that belong to each application	Application
Number of inbound 406 responses	<code>getTotalInboundResponses(applicationName, "406");</code>	Number of inbound 406 (Not Acceptable) responses that belong to each application	Application
Number of inbound 407 responses	<code>getTotalInboundResponses(applicationName, "407");</code>	Number of inbound 407 (Proxy Authentication Required) responses that belong to each application	Application
Number of inbound 408 responses	<code>getTotalInboundResponses(applicationName, "408");</code>	Number of inbound 408 (Request Timeout) responses that belong to each application	Application
Number of inbound 410 responses	<code>getTotalInboundResponses(applicationName, "410");</code>	Number of inbound 410 (Gone) responses that belong to each application	Application
Number of inbound 413 responses	<code>getTotalInboundResponses(applicationName, "413");</code>	Number of inbound 413 (Request Entity Too Large) responses that belong to each application	Application
Number of inbound 414 responses	<code>getTotalInboundResponses(applicationName, "414");</code>	Number of inbound 414 (Request URI Too Long) responses that belong to each application	Application
Number of inbound 415 responses	<code>getTotalInboundResponses(applicationName, "415");</code>	Number of inbound 415 (Unsupported Media Type) responses that belong to each application	Application
Number of inbound 416 responses	<code>getTotalInboundResponses(applicationName, "416");</code>	Number of inbound 416 (Unsupported URI Scheme) responses that belong to each application	Application

Table 179. SIP container inbound responses (continued). The object name of the MXBean from which the counters can be retrieved is: "WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse", "getTotalInboundResponses", _appName, "100")`.

This table lists the inbound response counters.

Name	Method	Description	Granularity
Number of inbound 420 responses	<code>getTotalInboundResponses(applicationName, "420");</code>	The number of inbound 420 (Bad Extension) responses that belong to each application	Application
Number of inbound 421 responses	<code>getTotalInboundResponses(applicationName, "421");</code>	The number of inbound 421 (Extension Required) responses that belong to each application	Application
Number of inbound 423 responses	<code>getTotalInboundResponses(applicationName, "423");</code>	The number of inbound 423 (Interval Too Brief) responses that belong to each application	Application
Number of inbound 480 responses	<code>getTotalInboundResponses(applicationName, "480");</code>	The number of inbound 480 (Temporarily Unavailable) responses that belong to each application	Application
Number of inbound 481 responses	<code>getTotalInboundResponses(applicationName, "481");</code>	The number of inbound 481 (Call Leg Done) responses that belong to each application	Application
Number of inbound 482 responses	<code>getTotalInboundResponses(applicationName, "482");</code>	The number of inbound 482 (Loop Detected) responses that belong to each application	Application
Number of inbound 483 responses	<code>getTotalInboundResponses(applicationName, "483");</code>	The number of inbound 483 (Too Many Hops) responses that belong to each application	Application
Number of inbound 484 responses	<code>getTotalInboundResponses(applicationName, "484");</code>	The number of inbound 484 (Address Incomplete) responses that belong to each application	Application
Number of inbound 485 responses	<code>getTotalInboundResponses(applicationName, "485");</code>	The number of inbound 485 (Ambiguous) responses that belong to each application	Application
Number of inbound 486 responses	<code>getTotalInboundResponses(applicationName, "486");</code>	The number of inbound 486 (Busy Here) responses that belong to each application	Application
Number of inbound 487 responses	<code>getTotalInboundResponses(applicationName, "487");</code>	The number of inbound 487 (Request Terminated) responses that belong to each application	Application
Number of inbound 488 responses	<code>getTotalInboundResponses(applicationName, "488");</code>	The number of inbound 488 (Not Acceptable Here) responses that belong to each application	Application

Table 179. SIP container inbound responses (continued). The object name of the MXBean from which the counters can be retrieved is: "WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse", "getTotalInboundResponses", _appName, "100")`.

This table lists the inbound response counters.

Name	Method	Description	Granularity
Number of inbound 491 responses	<code>getTotalInboundResponses(applicationName, "491");</code>	Number of inbound 491 (Request Pending) responses that belong to each application	Application
Number of inbound 493 responses	<code>getTotalInboundResponses(applicationName, "493");</code>	Number of inbound 493 (Undecipherable) responses that belong to each application	Application
Number of inbound 500 responses	<code>getTotalInboundResponses(applicationName, "500");</code>	Number of inbound 500 (Server Internal Error) responses that belong to each application	Application
Number of inbound 501 responses	<code>getTotalInboundResponses(applicationName, "501");</code>	Number of inbound 501 (Not Implemented) responses that belong to each application	Application
Number of inbound 502 responses	<code>getTotalInboundResponses(applicationName, "502");</code>	Number of inbound 502 (Bad Gateway) responses that belong to each application	Application
Number of inbound 503 responses	<code>getTotalInboundResponses(applicationName, "503");</code>	Number of inbound 503 (Service Unavailable) responses that belong to each application	Application
Number of inbound 504 responses	<code>getTotalInboundResponses(applicationName, "504");</code>	Number of inbound 504 (Server Timeout) responses that belong to each application	Application
Number of inbound 505 responses	<code>getTotalInboundResponses(applicationName, "505");</code>	Number of inbound 505 (Version Not Supported) responses that belong to each application	Application
Number of inbound 513 responses	<code>getTotalInboundResponses(applicationName, "513");</code>	Number of inbound 513 (Message Too Large) responses that belong to each application	Application
Number of inbound 600 responses	<code>getTotalInboundResponses(applicationName, "600");</code>	Number of inbound 600 (Busy Everywhere) responses that belong to each application	Application
Number of inbound 603 responses	<code>getTotalInboundResponses(applicationName, "603");</code>	Number of inbound 603 (Decline) responses that belong to each application	Application

*Table 179. SIP container inbound responses (continued).* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=InboundResponseCounters,name=SipContainer.InboundResponse", "getTotalInboundResponses", _appName, "100")`.

This table lists the inbound response counters.

Name	Method	Description	Granularity
Number of inbound 604 responses	<code>getTotalInboundResponses(applicationName, "604");</code>	The number of inbound 604 (Does Not Exit Anywhere) responses that belong to each application	Application
Number of inbound 606 responses	<code>getTotalInboundResponses(applicationName, "606");</code>	The number of inbound 606 (Not Acceptable Anywhere) responses that belong to each application	Application

*Table 180. SIP container outbound requests.* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=OutboundRequestCounters,name=SipContainer.OutboundRequest". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=OutboundRequestCounters,name=SipContainer.OutboundRequest", "getTotalOutboundRequests", _appName, "INVITE")`.

This table lists the outbound request counters.

Name	Method	Description	Granularity
Number of outbound NOT SIP STANDARD requests	<code>getTotalOutboundRequests(applicationName, "NOTSIPSTANDARD");</code>	The number of outbound NOT SIP STANDARD requests that belong to each application	Application
Number of outbound REGISTER requests	<code>getTotalOutboundRequests(applicationName, "REGISTER");</code>	The number of outbound REGISTER requests that belong to each application	Application
Number of outbound INVITE requests	<code>getTotalOutboundRequests(applicationName, "INVITE");</code>	The number of outbound INVITE requests that belong to each application	Application
Number of outbound ACK requests	<code>getTotalOutboundRequests(applicationName, "ACK");</code>	The number of outbound ACK requests that belong to each application	Application
Number of outbound OPTIONS requests	<code>getTotalOutboundRequests(applicationName, "OPTIONS");</code>	The number of outbound OPTIONS requests that belong to each application	Application
Number of outbound BYE requests	<code>getTotalOutboundRequests(applicationName, "BYE");</code>	The number of outbound BYE requests that belong to each application	Application
Number of outbound CANCEL requests	<code>getTotalOutboundRequests(applicationName, "CANCEL");</code>	The number of outbound CANCEL requests that belong to each application	Application
Number of outbound PRACK requests	<code>getTotalOutboundRequests(applicationName, "PRACK");</code>	The number of outbound PRACK requests that belong to each application	Application
Number of outbound INFO requests	<code>getTotalOutboundRequests(applicationName, "INFO");</code>	The number of outbound INFO requests that belong to each application	Application

*Table 180. SIP container outbound requests (continued).* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=OutboundRequestCounters,name=SipContainer.OutboundRequest". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=OutboundRequestCounters,name=SipContainer.OutboundRequest", "getTotalOutboundRequests", _appName, "INVITE").`

This table lists the outbound request counters.

Name	Method	Description	Granularity
Number of outbound SUBSCRIBE requests	<code>getTotalOutboundRequests(applicationName, "SUBSCRIBE");</code>	The number of outbound SUBSCRIBE requests that belong to each application	Application
Number of outbound NOTIFY requests	<code>getTotalOutboundRequests(applicationName, "NOTIFY");</code>	The number of outbound NOTIFY requests that belong to each application	Application
Number of outbound MESSAGE requests	<code>getTotalOutboundRequests(applicationName, "MESSAGE");</code>	The number of outbound MESSAGE requests that belong to each application	Application
Number of outbound PUBLISH requests	<code>getTotalOutboundRequests(applicationName, "PUBLISH");</code>	The number of outbound PUBLISH requests that belong to each application	Application
Number of outbound REFER requests	<code>getTotalOutboundRequests(applicationName, "REFER");</code>	The number of outbound REFER requests that belong to each application	Application
Number of outbound UPDATE requests	<code>getTotalOutboundRequests(applicationName, "UPDATE");</code>	The number of outbound UPDATE requests that belong to each application	Application

*Table 181. SIP container outbound responses.* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse", "getTotalOutboundResponses", _appName, "100").`

This table lists the outbound response counters.

Name	Method	Description	Granularity
Number of outbound 100 responses	<code>getTotalOutboundResponses(applicationName, "100");</code>	The number of outbound 100 (Trying) responses that belong to each application	Application
Number of outbound 180 responses	<code>getTotalOutboundResponses(applicationName, "180");</code>	The number of outbound 180 (Ringing) responses that belong to each application	Application
Number of outbound 181 responses	<code>getTotalOutboundResponses(applicationName, "181");</code>	The number of outbound 181 (Call being forwarded) responses that belong to each application	Application
Number of outbound 182 responses	<code>getTotalOutboundResponses(applicationName, "182");</code>	The number of outbound 182 (Call Queued) responses that belong to each application	Application

*Table 181. SIP container outbound responses (continued).* The object name of the MXBean from which the counters can be retrieved is: "WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse", "getTotalOutboundResponses", _appName, "100")`.

This table lists the outbound response counters.

Name	Method	Description	Granularity
Number of outbound 183 responses	<code>getTotalOutboundResponses("183");</code>	The number of outbound 183 (Session Progress) responses that belong to each application	Application
Number of outbound 200 responses	<code>getTotalOutboundResponses("200");</code>	The number of outbound 200 (OK) responses that belong to each application	Application
Number of outbound 202 responses	<code>getTotalOutboundResponses("202");</code>	The number of outbound 202 (Accepted) responses that belong to each application	Application
Number of outbound 300 responses	<code>getTotalOutboundResponses("300");</code>	The number of outbound 300 (Multiple choices) responses that belong to each application	Application
Number of outbound 301 responses	<code>getTotalOutboundResponses("301");</code>	The number of outbound 301 (Moved Permanently) responses that belong to each application	Application
Number of outbound 302 responses	<code>getTotalOutboundResponses("302");</code>	The number of outbound 302 (Moved Temporarily) responses that belong to each application	Application
Number of outbound 305 responses	<code>getTotalOutboundResponses("305");</code>	The number of outbound 305 (Use Proxy) responses that belong to each application	Application
Number of outbound 380 responses	<code>getTotalOutboundResponses("380");</code>	The number of outbound 380 (Alternative Service) responses that belong to each application	Application
Number of outbound 400 responses	<code>getTotalOutboundResponses("400");</code>	The number of outbound 400 (Bad Request) responses that belong to each application	Application
Number of outbound 401 responses	<code>getTotalOutboundResponses("401");</code>	The number of outbound 401 (Unauthorized) responses that belong to each application	Application
Number of outbound 402 responses	<code>getTotalOutboundResponses("402");</code>	The number of outbound 402 (Payment Required) responses that belong to each application	Application

*Table 181. SIP container outbound responses (continued).* The object name of the MXBean from which the counters can be retrieved is: "WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse", "getTotalOutboundResponses", _appName, "100")`.

This table lists the outbound response counters.

Name	Method	Description	Granularity
Number of outbound 403 responses	<code>getTotalOutboundResponses("403");</code>	Number of outbound 403 (Forbidden) responses that belong to each application	Application
Number of outbound 404 responses	<code>getTotalOutboundResponses("404");</code>	Number of outbound 404 (Not Found) responses that belong to each application	Application
Number of outbound 405 responses	<code>getTotalOutboundResponses("405");</code>	Number of outbound 405 (Method Not Allowed) responses that belong to each application	Application
Number of outbound 406 responses	<code>getTotalOutboundResponses("406");</code>	Number of outbound 406 (Not Acceptable) responses that belong to each application	Application
Number of outbound 407 responses	<code>getTotalOutboundResponses("407");</code>	Number of outbound 407 (Proxy Authentication Required) responses that belong to each application	Application
Number of outbound 408 responses	<code>getTotalOutboundResponses("408");</code>	Number of outbound 408 (Request Timeout) responses that belong to each application	Application
Number of outbound 410 responses	<code>getTotalOutboundResponses("410");</code>	Number of outbound 410 (Gone) responses that belong to each application	Application
Number of outbound 413 responses	<code>getTotalOutboundResponses("413");</code>	Number of outbound 413 (Request Entity Too Large) responses that belong to each application	Application
Number of outbound 414 responses	<code>getTotalOutboundResponses("414");</code>	Number of outbound 414 (Request URI Too Long) responses that belong to each application	Application
Number of outbound 415 responses	<code>getTotalOutboundResponses("415");</code>	Number of outbound 415 (Unsupported Media Type) responses that belong to each application	Application
Number of outbound 416 responses	<code>getTotalOutboundResponses("416");</code>	Number of outbound 416 (Unsupported URI Scheme) responses that belong to each application	Application

Table 181. SIP container outbound responses (continued). The object name of the MXBean from which the counters can be retrieved is: "WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse", "getTotalOutboundResponses", _appName, "100")`.

This table lists the outbound response counters.

Name	Method	Description	Granularity
Number of outbound 420 responses	<code>getTotalOutboundResponses("420");</code>	Number of outbound 420 (Bad Extension) responses that belong to each application	Application
Number of outbound 421 responses	<code>getTotalOutboundResponses("421");</code>	Number of outbound 421 (Extension Required) responses that belong to each application	Application
Number of outbound 423 responses	<code>getTotalOutboundResponses("423");</code>	Number of outbound 423 (Interval Too Brief) responses that belong to each application	Application
Number of outbound 480 responses	<code>getTotalOutboundResponses("480");</code>	Number of outbound 480 (Temporarily Unavailable) responses that belong to each application	Application
Number of outbound 481 responses	<code>getTotalOutboundResponses("481");</code>	Number of outbound 481 (Call Leg Done) responses that belong to each application	Application
Number of outbound 482 responses	<code>getTotalOutboundResponses("482");</code>	Number of outbound 482 (Loop Detected) responses that belong to each application	Application
Number of outbound 483 responses	<code>getTotalOutboundResponses("483");</code>	Number of outbound 483 (Too Many Hops) responses that belong to each application	Application
Number of outbound 484 responses	<code>getTotalOutboundResponses("484");</code>	Number of outbound 484 (Address Incomplete) responses that belong to each application	Application
Number of outbound 485 responses	<code>getTotalOutboundResponses("485");</code>	Number of outbound 485 (Ambiguous) responses that belong to each application	Application
Number of outbound 486 responses	<code>getTotalOutboundResponses("486");</code>	Number of outbound 486 (Busy Here) responses that belong to each application	Application
Number of outbound 487 responses	<code>getTotalOutboundResponses("487");</code>	Number of outbound 487 (Request Terminated) responses that belong to each application	Application

Table 181. SIP container outbound responses (continued). The object name of the MXBean from which the counters can be retrieved is: "WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse", "getTotalOutboundResponses", _appName, "100")`.

This table lists the outbound response counters.

Name	Method	Description	Granularity
Number of outbound 488 responses	<code>getTotalOutboundResponses("488");</code>	Number of outbound 488 (Not Acceptable Here) responses that belong to each application	Application
Number of outbound 491 responses	<code>getTotalOutboundResponses("491");</code>	Number of outbound 491 (Request Pending) responses that belong to each application	Application
Number of outbound 493 responses	<code>getTotalOutboundResponses("493");</code>	Number of outbound 493 (Undecipherable) responses that belong to each application	Application
Number of outbound 500 responses	<code>getTotalOutboundResponses("500");</code>	Number of outbound 500 (Server Internal Error) responses that belong to each application	Application
Number of outbound 501 responses	<code>getTotalOutboundResponses("501");</code>	Number of outbound 501 (Not Implemented) responses that belong to each application	Application
Number of outbound 502 responses	<code>getTotalOutboundResponses("502");</code>	Number of outbound 502 (Bad Gateway) responses that belong to each application	Application
Number of outbound 503 responses	<code>getTotalOutboundResponses("503");</code>	Number of outbound 503 (Service Unavailable) responses that belong to each application	Application
Number of outbound 504 responses	<code>getTotalOutboundResponses("504");</code>	Number of outbound 504 (Server Timeout) responses that belong to each application	Application
Number of outbound 505 responses	<code>getTotalOutboundResponses("505");</code>	Number of outbound 505 (Version Not Supported) responses that belong to each application	Application
Number of outbound 513 responses	<code>getTotalOutboundResponses("513");</code>	Number of outbound 513 (Message Too Large) responses that belong to each application	Application
Number of outbound 600 responses	<code>getTotalOutboundResponses("600");</code>	Number of outbound 600 (Busy Everywhere) responses that belong to each application	Application

*Table 181. SIP container outbound responses (continued).* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse". To retrieve the counters, use the JMXConnection.invoke method. For example, `_connection.invoke("WebSphere:type=OutboundResponseCounters,name=SipContainer.OutboundResponse", "getTotalOutboundResponses", _appName, "100")`.

This table lists the outbound response counters.

Name	Method	Description	Granularity
Number of outbound 603 responses	<code>getTotalOutboundResponses(applicationName, "603");</code>	The number of outbound 603 (Decline) responses that belong to each application	Application
Number of outbound 604 responses	<code>getTotalOutboundResponses(applicationName, "604");</code>	The number of outbound 604 (Does Not Exit Anywhere) responses that belong to each application	Application
Number of outbound 606 responses	<code>getTotalOutboundResponses(applicationName, "606");</code>	The number of outbound 606 (Not Acceptable Anywhere) responses that belong to each application	Application

*Table 182. SIP container task duration counters.* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=TaskDurationCounters,name=SipContainer.TaskDuration". To retrieve the attributes, use the JMXConnection.getAttribute method. For example: `_connection.getAttribute("WebSphere:type=TaskDurationCounters,name=SipContainer.TaskDuration", "AvgTaskDurationOutBoundQueue")`

This table lists the task duration module counters.

Name	Attribute/Method	Description	Granularity
Average Task Duration in outbound queue	<code>AvgTaskDurationOutBoundQueue</code>	The average task duration in the SIP stack outbound queue over a configured window of time	Server
Maximum Task Duration in outbound queue	<code>MaxTaskDurationOutBoundQueue</code>	The maximum task duration in the SIP stack outbound queue over a configured window of time	Server
Minimum Task Duration in outbound queue	<code>MinTaskDurationOutBoundQueue</code>	The minimum task duration in the SIP stack outbound queue over a configured window of time	Server
Average Task Duration in processing queue	<code>AvgTaskDurationInProcessingQueue</code>	The average task duration in the SIP container processing queue over a configured window of time	Server
Maximum Task Duration in processing queue	<code>MaxTaskDurationInProcessingQueue</code>	The maximum task duration in the SIP container processing queue over a configured window of time	Server
Minimum Task Duration in processing queue	<code>MinTaskDurationInProcessingQueue</code>	The minimum task duration in the SIP container processing queue over a configured window of time	Server

*Table 182. SIP container task duration counters (continued).* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=TaskDurationCounters,name=SipContainer.TaskDuration". To retrieve the attributes, use the JMXConnection.getAttribute method. For example:

```
_connection.getAttribute("WebSphere:type=TaskDurationCounters,name=SipContainer.TaskDuration", "AvgTaskDurationOutBoundQueue")
```

This table lists the task duration module counters.

Name	Attribute/Method	Description	Granularity
Average Task Duration in application code	getAvgTaskDurationInApplication(appName)	The average task duration in the SIP application code over a configured period	Application
Maximum Task Duration in application code	getMaxTaskDurationInApplication(appName)	The maximum task duration in the SIP application code over a configured period	Application
Minimum Task Duration in application code	getMinTaskDurationInApplication(appName)	The minimum task duration in the SIP application code over a configured period	Application

*Table 183. SIP container queue monitoring counters.* The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=QueueMonitoringModule,name=SipContainer.QueueMonitor". To retrieve the attributes, use the JMXConnection.getAttribute method. For example:

```
_connection.getAttribute("WebSphere:type=QueueMonitoringModule,name=SipContainer.QueueMonitor", "TotalTasksCountInProcessingQueue").
```

This table lists the queue monitoring counters.

Name	Attribute	Description	Granularity
Total number of tasks that have flowed through the processing SIP container queue	TotalTasksCountInProcessingQueue	The total number of tasks, such as messages or SIP timer events, that have flowed through the processing SIP container queue over a configured window of time	Server
Maximum number of tasks in the processing SIP container queue	PeakTasksCountInProcessingQueue	The maximum number of tasks in the processing SIP container queue over a configured window of time	Server
Minimum number of tasks in the processing SIP container queue	MinTasksCountInProcessingQueue	The minimum number of tasks in the processing SIP container queue over a configured window of time	Server
Maximum percent full of the processing SIP container queue	PercentageFullTasksCountInProcessingQueue	The maximum processing SIP container queue usage percentage over a configured window of time	Server
Total number of tasks that have flowed through the outbound SIP stack queue	TotalTasksCountInOutboundQueue	The total number of tasks that have flowed through the outbound SIP stack queue over a configured window of time	Server

Table 183. SIP container queue monitoring counters (continued). The object name of the MBean from which the counters can be retrieved is: "WebSphere:type=QueueMonitoringModule,name=SipContainer.QueueMonitor". To retrieve the attributes, use the JMXConnection.getAttribute method. For example:  
`_connection.getAttribute("WebSphere:type=QueueMonitoringModule,name=SipContainer.QueueMonitor", "TotalTasksCountInProcessingQueue").`

This table lists the queue monitoring counters.

Name	Attribute	Description	Granularity
Maximum number of tasks in the outbound SIP stack queue	PeakTasksCountInOutboundQueue	The maximum number of tasks in the outbound SIP stack queue over a configured window of time	Server
Minimum number of tasks in the outbound SIP stack queue	MinTasksCountInOutboundQueue	The minimum number of tasks in the outbound SIP stack queue over a configured window of time	Server
Maximum percent full of the outbound SIP stack queue	PercentageFullTasksCountInOutboundQueue	The maximum outbound SIP stack queue usage percentage over a configured window of time	Server

---

## Liberty:Sessions monitoring

### 8.5.5.0

You can use the SessionStats MBean to monitor the performance data of sessions in Liberty.

The performance data of sessions for each application is available as an MBean, which can be accessed through JMX.

The sessions that are associated with a single web application have their own SessionStats MBean (that is, one SessionStats MBean for each web application).

The ObjectName for identifying each Session MBean is:

`WebSphere:type=SessionStats,name=*`

For example:

`WebSphere:type=SessionStats,name=default_host/trade_lite`

`WebSphere:type=SessionStats,name=default_host/moneybank`

The MBean is responsible for reporting SessionStats for a single web application. The following key data is available for the SessionStats MBean after monitoring is enabled:

#### CreateCount

The total number of sessions created.

#### LiveCount

The total number of sessions that are currently cached in memory.

#### ActiveCount

The total number of concurrently active sessions. A session is active if Liberty is processing a request that uses that session.

#### InvalidatedCount

The total number of sessions that are invalidated.

## InvalidatedCountbyTimeout

The total number of sessions invalidated by a timeout.

---

## Liberty:ConnectionPool monitoring

### 8.5.5.0

You can use the ConnectionPool MBean for ConnectionPool monitoring of Liberty.

Performance data is made available for each ConnectionPool. Connection pools manage connections from data sources and connection factories.

Each connection manager has a ConnectionPool MBean associated with it, and there is one MBean for every connection manager.

The ObjectName for identifying each ConnectionPool MBean is:

```
WebSphere:type=ConnectionPoolStats,name=<IDENTIFIER_OF_CONNECTION_MANAGER>
```

The following example shows a connection pool (for a data source or connection factory) that does not have a JNDI name. The data source [default-x] name is considered as the data source object when JNDI is not specified.

```
WebSphere:type=ConnectionPoolStats,name=transaction/dataSource[default-0]/connectionManager
```

```
<transaction enableLoggingForHeuristicReporting="true" transactionLogSize="2048">
  <dataSource transactional="false">
    <jdbcDriver libraryRef="DerbyLib"/>
    <properties.derby.embedded databaseName="<DIR Path>/<DatabaseName>" createDatabase="create"/>
  </dataSource>
</transaction>
```

Example configurations when connection manager is provided

- When an explicit ID is not specified, an ID is generated based on its parent

```
WebSphere:type=ConnectionPoolStats,name=dataSource[MyDataSource]/connectionManager[default-0]
```

```
<dataSource id="MyDataSource">
  <connectionManager maxPoolSize="10"/>
  <jdbcDriver libraryRef="DB2JCC4LIB"/>
  <properties.db2.jcc .../>
</dataSource>
```

- When an ID is specified, that becomes the identifier

```
WebSphere:type=ConnectionPoolStats,name=connectionManager[Pool2]
```

```
<dataSource id="DataSource2" jdbcDriverRef="DB2JCCDriver" connectionManagerRef="Pool2">
  <properties.db2.jcc .../>
</dataSource>
<connectionManager id="Pool2" maxPoolSize="20"/>
```

- Obtaining the correct identifier for a type 2 driver connection pool.
  - Ensure that the application that is using the pool makes a call to DB2 so that the pool is initialized.
  - Navigate to the REST interface to determine the proper identifier to use in the configuration. For example:

```
host:443/IBMJMXConnectorREST/mbeans
```

Specifying the correct identifier for a connection pool for a type 2 driver

```
{ "objectName": "WebSphere:type=ConnectionPoolStats,name=jdbc/acp01", "
  className": "com.ibm.ws.connectionpool.monitor.ConnectionPoolStats", "
  URL": "/IBMJMXConnectorREST/mbeans/WebSphere%3Aname%3Djdbc%2Facp01%
  2Ctype%3DConnectionPoolStats" }
```

The ConnectionPool MBean is responsible for reporting ConnectionPool Stats for a single connection manager. The following counter attributes are available for the ConnectionPool MBean after monitoring is enabled:

#### CreateCount

The total number of connections created.

#### DestroyCount

The total number of connections destroyed.

#### ManagedConnectionCount

The number of ManagedConnection objects that are in use.

#### WaitTime

The average waiting time in milliseconds until a connection is granted.

#### ConnectionHandleCount

The number of Connection objects that are in use.

#### FreeConnectionCount

The number of free connections in the pool.

---

## Liberty:Multiple components monitoring

### 8.5.5.0

You can filter the components that you want to monitor by using the monitor-1.0 feature in Liberty. The components to be filtered must be configured in the server.xml file.

1. To specify the components that you want to filter, add the following code to the server.xml file.

```
<server description="new server">
    <featureManager>
        <feature>jsp-2.2</feature>
        <feature>jdbc-4.0</feature>
        <feature>monitor-1.0</feature>
    </featureManager>
    <monitor filter="JVM,ThreadPool,WebContainer,Session,ConnectionPool"/>
</server>
```

By default, if the filters are not provided in the <monitor> tag, all the components that are currently monitored as part of the monitor-1.0 feature are monitored. You can specify the components that you want to monitor by providing the group name as part of the filter.

For example: If you want to monitor only the *JVM* and *WebContainer* components, specify the components in the server.xml file as follows:

```
<monitor filter="JVM,WebContainer"/>
```

2. To remove components from monitoring.

To stop monitoring a component, you must remove the component from the filter group at run time.

For example: The following filter configuration monitors the *JVM*, *ThreadPool*, *WebContainer*, *Session* and *ConnectionPool* components:

```
<monitor filter="JVM,ThreadPool,WebContainer,Session,ConnectionPool"/>
```

To stop monitoring the components *WebContainer* and *Session*, remove those components from the filter configuration:

```
<monitor filter="JVM,ThreadPool,ConnectionPool" />
```

3. To enable monitoring of components at run time.

If you want to enable monitoring for specific components at run time, you can specify the components in the monitor tag at run time.

The data that is collected by the filtering components is available as MXBeans. For more information about the various MXBeans, see Chapter 11, "Monitoring the Liberty server runtime environment," on page 2267.

**Note:** **8.5.5.0** Currently, fine-grained monitoring is supported only at the component level (such as *WebContainer*, *ThreadPool*, *JVM*) and not at the counter level.

---

## Liberty:HTTP access logging

You can configure access log settings for HTTP endpoints.

### HTTP access log settings

An HTTP access log contains a record of all inbound client requests handled by HTTP endpoints. You can enable access logging in the HTTP server, or you can enable it in the Liberty server in two modes: one log common to multiple endpoints, or one log for each endpoint.

**Note:** If you do not specify attributes, the defaults are used. To see a list of the default attributes, see `httpAccessLogging` in the list of liberty configuration elements: .

- Using a common log

To enable logging for multiple endpoints using common settings, include *httpAccessLogging* as a top-level element in your `server.xml` file, and then reference it from multiple `httpEndpoint` elements:

```
<httpAccessLogging id="accessLogging"/>
<httpEndpoint id="defaultHttpEndpoint" accessLoggingRef="accessLogging"/>
<httpEndpoint id="otherHttpEndpoint" accessLoggingRef="accessLogging" httpPort="9081" httpsPort="9444"/>
```

- Using distinct logs for each endpoint

To enable logging for individual endpoints, use an *accessLogging* child element and specify a file path that does not conflict with other logs:

```
<httpEndpoint id="defaultHttpEndpoint">
  <accessLogging filepath="${server.output.dir}/logs/http_defaultEndpoint_access.log"/>
</httpEndpoint>
```

- Using logs for the HTTP server

For a list of the available HTTP server side properties and their descriptions, see Apache Module `mod_log_config`.

### HTTP access log format

For a list of the available log format properties and their descriptions, see the *accessLogFormat* configuration for WebSphere Application Server traditional in HTTP transport channel custom properties. This log format string is specified using the *logFormat* attribute of `httpAccessLogging` or `accessLogging` elements in `server.xml`:

```
<httpAccessLogging logFormat='%h %u %{t}W "%r" %s %b' />
```

or

```
<httpEndpoint id="defaultHttpEndpoint">
  <accessLogging filepath="${server.output.dir}/logs/http_defaultEndpoint_access.log"
    logFormat='%h %i %u %t "%r" %s %b' />
</httpEndpoint>
```



---

## Chapter 12. Tuning Liberty

You can tune parameters and attributes of Liberty.

### About this task

Liberty supports different attributes in the `server.xml` file to influence application performance. You can use these parameters and attributes to achieve better performance. To tune Liberty for secure applications, see [Tuning Liberty for secure applications](#).

### Procedure

- Tune the JVM.

Tuning the JVM is a most important tuning step whether you configure a development or production environment. When you tune the JVM for Liberty, use the `jvm.options` file in the `${server.config.dir}` directory. You can specify each of the JVM arguments that you want to use, one option per line. For more information, see “Customizing the Liberty environment” on page 1565. An example of the `jvm.options` file is as follows:

```
-Xms50m  
-Xmx256m
```

For a development environment, you might be interested in faster server startup, so consider setting the minimum heap size to a small value, and the maximum heap size to whatever value is needed for your application. For a production environment, setting the minimum heap size and maximum heap size to the same value can provide the best performance by avoiding heap expansion and contraction.

- Tune transport channel services.

The transport channel services manage client connections, I/O processing for HTTP, thread pools, and connection pools. For applications on Liberty, the following attributes are available for different elements that can be used to improve runtime performance, scalability, or both. For each of these attributes, see .

#### **maxKeepAliveRequests of httpOptions**

This option specifies the maximum number of persistent requests that are allowed on a single HTTP connection if persistent connections are enabled. A value of `-1` means unlimited. This option supports low latency or high throughput applications, and SSL connections for use in situations where building up a new connection can be costly. Here is an example of how you code this option in the `server.xml` file:

```
<httpOptions maxKeepAliveRequests="-1" />
```

#### **maxPoolSize of connectionManager**

This option specifies the maximum number of physical connections for the connection pool. The default value is 50. The optimal setting here depends on the application characteristics. For an application in which every thread obtains a connection to the database, you might start with a 1:1 mapping to the `coreThreads` attribute. Here is an example of how you code this option in the `server.xml` file:

```
<connectionManager ... maxPoolSize="40" />
```

#### **purgePolicy of connectionManager**

This option specifies which connections to destroy when a stale connection is detected in a pool. The default value is the entire pool. It might be better to purge only the failing connection. Here is an example of how you code this option in the `server.xml` file:

```
<connectionManager ... purgePolicy="FailingConnectionOnly" />
```

#### **numConnectionsPerThreadLocal of connectionManager**

This option specifies the number of database connections to cache for each executor thread.

This setting can provide a major improvement on large multi-core (8+) machines by reserving the specified number of database connections for each thread.

Using thread local storage for connections can increase performance for applications on multi-threaded systems. When you set **numConnectionsPerThreadLocal** to 1 or more, these connections per thread are stored in thread local storage. When you use **numConnectionsPerThreadLocal**, consider two other values:

- The number of application threads
- The connection pool maximum connections

For best performance, if you have *n* applications threads, you must set the maximum pool connections to at least *n* times the value of the **numConnectionsPerThreadLocal** attribute and you must use the same credentials for all connection requests. For example, if you use 20 application threads, set the maximum pool connections to 20 or more; If you set the value of **numConnectionsPerThreadLocal** attribute as 2 and there are 20 application threads, set the maximum pool connection to 40 or more. Here is an example of how you code this option in the `server.xml` file:

```
<connectionManager ... numConnectionsPerThreadLocal="1" />
```

#### **statementCacheSize of dataSource**

This option specifies the maximum number of cached prepared statements per connection. To set this option, complete the following prerequisite:

- Review the application code (or an SQL trace that you gather from the database or database driver) for all unique prepared statements.
- Ensure that the cache size is larger than the number of statements.

Here is an example of how you code this option in the `server.xml` file:

```
<dataSource ... statementCacheSize="60" >
```

#### **isolationLevel of dataSource**

The data source isolation level specifies the degree of data integrity and concurrency, which in turns controls the level of database locking. Four different options are available as following in order of best performing (least integrity) to worst performing (best integrity).

##### **TRANSACTION\_READ\_UNCOMMITTED**

Dirty reads, non-repeatable reads, and phantom reads can occur.

##### **TRANSACTION\_READ\_COMMITTED**

Dirty reads are prevented; non-repeatable reads and phantom reads can occur.

##### **TRANSACTION\_REPEATABLE\_READ**

Dirty reads and non-repeatable reads are prevented; phantom reads can occur.

##### **TRANSACTION\_SERIALIZABLE**

Dirty reads, non-repeatable reads, and phantom reads are prevented.

Here is an example of how you code this option in the `server.xml` file:

```
<dataSource ... isolationLevel="TRANSACTION_READ_COMMITTED">
```

- **8.5.5.6** Tune the default executor.

The Liberty default executor is self-tuning and adapts to the current workload by dynamically adding or removing threads. For most workloads, the executor does not require any tuning, and you are advised not to change any settings of the executor unless you encounter specific problems with thread creation.

If necessary, you can configure the **coreThreads** and **maxThreads** parameters of the executor element in the `server.xml` file to set lower and upper bounds for the Liberty auto-tuning code. The **coreThreads** setting is not usually needed because the executor contains aggressive anti-deadlocking code that adds threads to break the executor out of deadlock scenarios. Rarely, the anti-deadlocking code adds more

threads than are required. In this situation, you can use the **maxThreads** parameter of the executor element to cap the number of threads the executor is allowed to create.

- Decrease response time of servlets.

To decrease response time of servlets, add the following attribute to the `server.xml` file:

```
<webContainer skipMetaInfResourcesProcessing="true"/>
```

- Reduce idle server CPU time.

To reduce idle server CPU time, add the following attributes to the `server.xml` file:

```
<applicationMonitor dropinsEnabled="false" updateTrigger="disabled"/>
<config updateTrigger="disabled"/>
```

When the attributes are added, your server no longer monitors for configuration or application updates.

For more information about the configuration element descriptions, see .

- **8.5.5.7** Tuning startup time.

### CDI 1.2

By default, the CDI 1.2 feature scans all application archives. The CDI 1.2 feature can increase startup time substantially and have the most effect on larger applications. Implicit archive scanning for annotations can be disabled by setting **enableImplicitBeanArchives** value to `false`. This setting skips the scanning of archives unless they contain a `beans.xml` file.

```
<cdi12 enableImplicitBeanArchives="false"/>
```

**Note:** The `cdi-1.2` feature may be included even if its not in the `<features>` section of your `server.xml` file because other features, such as `webProfile-7.0` and `javaee-7.0`, include the `cdi-1.2` feature. Look in the `messages.log` file for "The server installed the following features:" to see if `cdi-1.2` was installed.

---

## Tuning Liberty for secure applications

You can tune Liberty to maximize the performance for secure applications.

### About this task

When you are securing your WebSphere application environment, it is important to understand the impact security can have on performance. Within an application server environment, running applications with security settings can often decrease performance because of increased processor usage from security tasks such as encryption, authentication, and authorization. These services can often increase the path length of application server requests, requiring more resources for each request and slowing down application throughput.

In most cases, you can reduce or eliminate some of this security-related performance loss through performance tuning. You can adjust the resources that are used by security services and choose to use only the security services that are required by a particular application or environment. Achieving the best possible performance, without sacrificing any necessary security, requires an understanding of your network topology and the security needs of your applications.

### Procedure

- Choose the connections that you want to encrypt.

In a WebSphere Application Server environment, you can encrypt the following transports:

- HTTP traffic that is to the web server
- HTTP traffic that is from the web server to the application server
- SOAP/JMX traffic
- File transfer service

– Web services over HTTP

When you are determining which traffic to transport over encrypted connections, consider whether the network that is connecting the communicating machines is private or public. There is a significant amount of resources that are associated with setting up a secured connection and encrypting and decrypting the traffic over that connection. You can make significant performance improvements by not requiring encryption over a secured network, for instance. If your application does not require that traffic is encrypted from the client to the HTTP server and from the HTTP server to the application Server, you might be able to use SSL only from the client to the HTTP server and therefore reduce resources that are required by security.

- Enable on-chip Advanced Encryption Standard (AES) Encryption.

If you are using IBM® SDK Java Technology Edition Version 7, Service Refresh 3 or later, and you are running on an Intel processor that supports the Advanced Encryption Standard (AES) New Instructions (AES-NI) instruction set, you can achieve performance improvement by taking advantage of on-chip AES encryption. Using these features, you can run AES encryption and decryption using hardware instructions without extra software.

To enable AES-NI usage, add the following property to the JVM command line or `jvm.options` file:

```
com.ibm.crypto.provider.doAESInHardware=true
```

Add the following property to the JVM command line or the `jvm.options` file to verify that the processor supports AES-NI instruction set:

```
com.ibm.crypto.provider.AESNITrace=true
```

For more information, see Intel Advanced Encryption Standard New Instructions.

- Choose your cipher key length.

In some cases, the bit length of a cipher key is governed by regulations that are put on the transfer of certain types of data. In these cases, the cipher and key length that you choose for a particular SSL connection can be predetermined. For situations where the key length is not regulated, you must choose the appropriate resources to allocate to security so that performance is not decreased more than is necessary. For example, a 256-bit cipher offers stronger encryption than a corresponding 128-bit cipher. However, decrypting messages with a stronger cipher requires more processing time.

When you are making your decision about the encryption strength to choose, consider the type of data that is traveling across a network. For example, sensitive information, such as financial or medical records, needs the maximum amount of security. Also, consider who has access to the network. If the network is protected by a firewall, consider decreasing the strength of the cipher, or possibly transmitting the data over an decrypted connection.

For more information about configuring SSL settings on Liberty, see “Liberty:SSL configuration attributes” on page 1835

- Set connection keep-alive requests.

In the Secure Socket Layer (SSL) protocol, the initial handshake uses a public-key cipher to exchange a private key for a faster private-key cipher. This faster cipher is used to encrypt and decrypt communication beyond the initial handshake. Because the cipher used for subsequent communication is faster than the one used for the initial handshake, it is important from a performance perspective to limit the number of SSL handshakes that are performed within the application server. You can achieve this result by increasing the length of an SSL connection by increasing session affinity.

One way to increase the duration of a single SSL connection is to enable persistent HTTP keep-alive connections. Increasing the duration prevents SSL handshakes from taking place on consecutive requests. You can make sure that persistent connections are enabled by verifying that the `keepAliveEnabled` attribute in the `httpOptions` element is set to `true` in the `server.xml` file. The default value is `true`.

Another way to tune persistent connections is by setting the maximum number of consecutive requests on a single HTTP connection. If your clients are making more than 100 requests consecutively, consider increasing the value of the `maxKeepAliveRequests` attribute in the `httpOptions` element in the `server.xml` file. The default value is 100.

For more information, see .

- Set the authentication cache settings.

Because the creation of an authentication subject can increase processor usage, Liberty provides an authentication cache to store a subject after the authentication of a user is successful. To fully take advantage of this service to increase performance, you must make sure that it is turned on and tuned according to your users and applications.

- Make sure that you do not disable the authentication cache. By default, the authentication cache is enabled to help improve performance.
- Consider changing the authentication cache timeout value. Increasing the timeout value enables subjects to remain in the authentication cache longer and reduces the number of reauthentications needed. However, increasing the timeout value increases the risk of user permissions becoming stale compared to a modified external repository, such as LDAP. Set your authentication cache timeout to reflect the estimated length of client sessions. You can specify the cache timeout by setting the value of the timeout attribute to whichever time you choose in the authCache element in the server.xml file. The default value is 600 seconds.
- Finally, if you are experiencing authentication times longer than expected, or you are noticing more traffic to an external authentication repository than expected, the authentication cache might be full. When the authentication cache is full, subjects are evicted. There is not a one-to-one mapping of authenticated users to authentication cache entries. The number of entries in the cache per user depends on other security configurations. It is a best practice for the maximum size of the authentication cache to be larger than the number of distinct authenticated users that are accessing the server at one time. Setting the maximum size of the authentication cache this way helps prevent subjects from being evicted from the cache before timing out. You can change the maximum size of the authentication cache by setting the value of the maxSize attribute in the authCache element in the server.xml file. The default size is 25000.

For more information, see “Configuring the authentication cache in Liberty” on page 1867.

- Configure the HTTP session affinity settings.

One of the operations in a secure application environment that drains performance the most is the initial setup, including the SSL handshake and authentication. In clustered environments, performance decreases might occur when a web client accesses different application servers. To prevent the increased processor usage of the SSL handshake and reauthentication, it is important to make sure that HTTP session affinity is configured.

HTTP session affinity ensures that consecutive client requests are routed to the same application server. HTTP session affinity aids performance in various ways, but specifically, it prevents the increased processor usage of reauthentication and SSL handshaking. Consult the documentation of your HTTP Server or Load Balancer for instructions on setting up HTTP session affinity.

For more information, see “Configuring session persistence for Liberty” on page 1610.

---

## Tuning federated LDAP repositories in Liberty

### 8.5.5.1

You can improve the performance of the federated LDAP repositories by monitoring and adjusting the cache and the context pool elements in the server.xml file.

#### About this task

The cached query results of the LDAP repositories save time, because the data need not be retrieved from the back-end server every time an LDAP operation is performed. The LDAP cache attributes are stored in the <ldapCache> element for quicker access. You must monitor the status of the cache and adjust the cache control parameters to improve the performance of the cache. The context pooling parameters can be adjusted to improve the performance of concurrent accesses to the LDAP servers.

## Procedure

- Configure the <ldapCache> element in the server.xml file.

Specify the LDAP cache control parameters to improve the performance:

### attributesCache

<size>: Specifies the number of entities that are stored in the cache. You can increase the size of the cache based on your business requirement, for example, increase the cache size if more number of entities are required in a business scenario.

<timeout>: Specifies how long the results can be cached before they are invalidated. If the back-end LDAP data is refreshed frequently to maintain an up-to-date cache, set a lesser timeout duration value.

<sizeLimit>: Specifies the maximum number of LDAP attributes per entity that can be stored in the cache. If an entity is associated with many attributes, increase the <sizeLimit> value.

### searchResultSizeLimit

Specifies the maximum number of search results that can be stored in the cache. Use the parameters in the <searchResultSizeLimit> element to tune the search results that are returned as part of the query.

- Configure the <contextPool> element parameters in the server.xml file to improve the performance of concurrent access to an LDAP server.

You can adjust the following parameters in the <contextPool> element to control the cache:

### contextPool

<initialSize>: Specifies the initial size of the context pool. The value must be set based on the load on the repository. If the initial number of requests to the LDAP server is expected to be high, increase the value of the initial size.

<maxSize>: Specifies the maximum context pool size. The value must be set based on the load on the repository. If you want to restrict the number of connections to the LDAP server, then set the value of the <maxSize> element to less than half of the maximum number of connections that the LDAP server can handle.

<timeout>: Specifies the duration after which the context pool times out. Specify a shorter timeout value so that fresh connections can be made to the LDAP server after the specified duration is timed out. For example, if the established connection is timed out after the configured interval, then set a shorter duration than the firewall timeout duration so that the connection is re-established.

<waitTime>: Specifies the waiting time before the context pool times out. If the value specified is high, then the time that is taken to establish a connection to the LDAP server is increased accordingly.

For more information about the <ldapCache> and <contextPool> elements, see

---

## Chapter 13. Liberty: Troubleshooting tips

Tips for troubleshooting Liberty.

To help you identify and resolve problems, the product has a unified logging component. See “Liberty: Logging and Trace” on page 2313. You can also use the IBM Support Assistant Data Collector (ISADC) command tool in the `${wlp.install.dir}/bin` directory to quickly collect diagnostic files, such as log files, configuration files or to run traces.

If you receive an exception message, information about the message is available in “Liberty: Messages” on page 2344.

The Java API documentation for each Liberty API is available in a separate .zip file in one of the javadoc subdirectories of the `${wlp.install.dir}/dev` directory.

**Distributed operating systems** Details of the main known restrictions that apply when you use Liberty are provided in the following two topics:

- “Liberty: Runtime environment known issues and restrictions” on page 2333.
- **Distributed operating systems** “Liberty: Developer Tools known issues and restrictions” on page 2342.

**z/OS** **IBM i** For details of the main known restrictions that apply when using Liberty, see “Liberty: Runtime environment known issues and restrictions” on page 2333.

Here is a set of tips to help you troubleshoot commonly experienced problems:

- Troubleshooting JDKs
- “Troubleshooting security” on page 2298
- “Troubleshooting LDAP” on page 2300
- “Troubleshooting SSL” on page 2300
- “Troubleshooting CORBA/IIOP” on page 2301
- “Troubleshooting logging and tracing” on page 2302
- “Troubleshooting JAX-WS” on page 2302
- “Troubleshooting WS-Security” on page 2306
- **Distributed operating systems** **IBM i** “Applying fix packs and interim fixes to an archive install” on page 2308
- “Troubleshooting performance” on page 2308
- **8.5.5.7** Troubleshooting SAML

### Check that your JDKs are at a supported level

If you experience problems that are not readily explained, check that the JDKs you are using are compliant with Java Version 6 or later, and are at a current service level. See “Minimum supported Java levels” on page 2333.

**Note:** A deadlock can occur when using Oracle based JVMs using Java Version 6. If you are using an affected JVM or JDK, the following settings can help prevent the deadlock from occurring:

- Enable the following VM option: `-XX:+UnlockDiagnosticVMOptions -XX:+UnsyncloadClass`
- Set the Equinox framework option to use classname locking for classloading by setting the following Equinox configuration option: `-Dosgi.classloader.lock=classname`

These can be set in a Java properties file, for example `jvm.options`, when starting the Liberty server.

## Troubleshooting security

This section describes some common security problems and solutions you can choose.

### **SESN0008E: A user authenticated as anonymous has attempted to access a session owned by user:LdapRegistry/cn=steven,o=myCompany,c=US.**

This error happens when an unauthenticated user tries to access a session created by an authenticated user. Session security that is enabled by default prevents unauthorized access of the sessions. Only the user who created a session can access it. See session security for more information.

This error can happen when you use a JSP (login.jsp for example) for your form-login and the SSO token sent by the browser is expired. Because the SSO token is expired, the user is prompted to log in again using the login.jsp page configured for the form-login. The jsp page, by default, tries to get a session. This session was originally created by the user whose token is expired. However, the token is expired and the user is not authenticated, no credentials are established when accessing this session that results in this error.

To avoid this error, restart the browser that starts a new session, or configure the login.jsp file to not create the session by default. If you choose to update the login.jsp file, set `<%@ page session="false" %>`.

### **CWWKS9104A: Authorization failed for user {0} while invoking {1} on {2}. The user is not granted access to any of the required roles: {3}.**

This error occurs when you do not have authorization to the roles required by the application. Make sure that the user or the group it belongs to is mapped to at least one of the roles that are mentioned in the error message. A user-to-role mapping defined in the `ibm-application-bnd.xml` file takes precedence over a mapping defined in the `server.xml` file. Check both resources to ensure that the correct mapping is defined. See “Configuring authorization for applications in Liberty” on page 1939.

### **CWWKS9104A: Authorization failed for user {0}.**

This error can occur if you specify both an application and webApplication for the same context root. If a conflict happens the latest configuration that is defined is ignored and causes an unexpected error, such as CWWKS9104A.

### **CWWKZ0013E: It is not possible to start two applications called {0} followed by unexpected security behavior and error messages such as CWWKS9104A.**

This error occurs when you specify your application in both the `server.xml` by using the application element and in the `dropins` folder. As a result, the application is attempted to be installed twice and the security configuration in the `server.xml` file might or might not take effect. To fix this, you must remove your application from the `dropins` folder and copy it to another directory. If you have to leave it in the `dropins` folder, you must disable the application monitoring by using the following code in your `server.xml` file:

```
<applicationMonitor dropinsEnabled="false"/>
```

### **An unauthenticated user was able to access my servlet or JSP.**

A user with a principal of **UNAUTHENTICATED** (or the unauthenticated SAF user on z/OS) is created when authentication fails or when your servlet or JSP is unprotected. An unauthenticated user can access your servlet or JSP if you do not define any security constraints or if you map the **EVERYONE** special subject to the role required by your application. Review the user-to-role mappings in the `ibm-application-bnd.xml/xml` and `server.xml` files. Take one of the following options:

- If your servlet or JSP is unprotected, add security constraints to the deployment descriptor of your application. See “Liberty:Authentication” on page 976.
- If you do not want any unauthenticated user to access your application, remove the **EVERYONE** special subject from the mapping for that role. See “Configuring authorization for applications in Liberty” on page 1939.

- If a certain user cannot be authorized to your servlet or JSP, review who is mapped to that role by examining the `ibm-application-bnd.xml/xml` and `server.xml` files. You can map a role to a user, group, or special subject. If your role is mapped to the **EVERYONE** special subject, any user is granted access. If your role is mapped to the **ALL\_AUTHENTICATED** special subject, any authenticated user is granted access. Remove these special subjects if you want to further limit who can access your servlet or JSP. Finally, check what group the user belongs to. Although the user might not have explicit access, the group might be mapped to the role. In this case, remove the user from the authorized group or remove the group from role mapping. See “Configuring authorization for applications in Liberty” on page 1939.

### Single sign-on (SSO) does not work.

If SSO does not work, make sure that the different Liberty servers that use the same LTPA keys, password, and `ssoCookieName` attribute of `webAppSecurity` element have the same Universal Time (UTC) and share the same user registry. Also, if the token expires or if the cookie is sent from a web browser after changing the user registry in a manner that is inconsistent, such as modifying the realm or removing the user the cookie represents, the SSO fails and the user is prompted to enter the credential information again. See “Customizing SSO configuration using LTPA cookies in Liberty” on page 1887.

### Debugging security public APIs.

`WSSecurityHelper` and `RegistryHelper` are loaded even if security is not enabled, for example, if a security feature - `appSecurity-1.0,appSecurity-2.0` or `zosSecurity-1.0` - is not specified. If security is not enabled, then `WSSecurityHelper.isServerSecurityEnabled()` and `WSSecurityHelper.isGlobalSecurityEnabled()` methods both return false, and `RegistryHelper.getUserRegistry()` method returns null.

Other security public API classes might not be loaded if security is not enabled. If you try to access these classes and call a method on one of these classes, you might get a `java.lang.NoClassDefFoundError` exception.

To avoid getting `java.lang.NoClassDefFoundError` exceptions, you must first test to see whether security is enabled by calling the `WSSecurityHelper.isServerSecurityEnabled()` or `WSSecurityHelper.isGlobalSecurityEnabled()` class, and then call other security public API classes only when security is enabled. See “Liberty:Security public APIs” on page 1004 for examples of this coding technique.

**Note:** This behavior is different from the traditional. In traditional, all classes are always loaded regardless of whether security is enabled or not.

### Cannot authenticate users with Unicode characters

In order to authenticate users whose names contain Unicode characters, you must set the character encoding type used by the Liberty server to UTF-8 by adding the following `jvm` option to the server start command:

```
-Dclient.encoding.override=UTF-8
```

You must also specify the `charset` and `pageEncoding` in your login page. Here is an example for specifying these parameters on a login JSP page:

```
<%@page contentType="text/html"; charset=UTF-8" pageEncoding="UTF-8"%>
```



### 8.5.5.4 `java.lang.annotation.AnnotationFormatError: java.lang.IllegalArgumentException:Wrong type at constant pool index at sun.reflect.annotation.AnnotationParser.parseAnnotations(AnnotationParser.java:87)`

This error can occur when an OpenID Connect or OAuth provider uses a Database Store for client registration with some JDK 7 versions.

To avoid this problem, upgrade to JDK version 7.1.

## Troubleshooting LDAP

This section describes some common LDAP problems and solutions you can choose.

**FFDC1015I: An FFDC Incident has been created: javax.naming.ServiceUnavailableException: myldapserver.mycompany.com:636; socket closed  
com.ibm.ws.security.registry.ldap.internal.LdapRegistry 298**

This message in messages.log indicates that the configured LDAP server cannot be reached. Check your LDAP server to verify that it is running and that its IP address can be accessed from Liberty server.

**The javax.naming.CommunicationException: simple bind failed: myldapserver.mycompany.com:636 [Root exception is javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.g: PKIX path building failed: java.security.cert.CertPathBuilderException: unable to find valid certification path to requested target]**

If you enable SSL on your LDAP server without copying the signer of the LDAP server into the truststore referenced in the LDAPSSLSettings element, a connection with the LDAP server fails with an SSL handshake error. Make sure that you copy the signer of the LDAP server into your truststore.

**The javax.naming.CommunicationException: myldapserver.mycompany.com:389 [Root exception is java.net.BindException: Address already in use: connect]**

This message might appear in the FFDC logs and indicates that the usable sockets on the local server are exhausted, which can result in a failure when connecting to your LDAP server. Make sure that the socket is not used and try again.

**CWWKS1100A: Authentication did not succeed for user ID xxxxx. An invalid user ID or password was specified**

This FFDC exception might happen on the server even though the user mentioned in the message is a valid user on the LDAP server under heavy load. With the LDAP configuration, you can add the reuseConnection=false property or disable it by using the developer tools. To fix the problem, set this property to the default value of true.

## Troubleshooting SSL

This section describes some common SSL problems and solutions you can choose.

**CWWKS9105E: Could not determine the SSL port for automatic redirection.**

This error occurs when you try to access an application that redirects to an SSL port and the SSL port is not available. The port might not be available because of a missing SSL configuration or some error in the SSL configuration definition. Check the SSL configuration in the server.xml file to make sure that it exists and is correct. See "Securing communications in Liberty" on page 1833.

**FFDC1015I: An FFDC Incident has been created: "java.lang.IllegalArgumentException: Unknown, incomplete configuration: missing id field  
com.ibm.ws.config.internal.cm.ManagedServiceFactoryTracker aSyncReadNupdate. Exception thrown while trying to read configuration and update ManagedServiceFactory. Exception = java.lang.IllegalArgumentException: Unknown, incomplete configuration: missing id field" at  
ffdc\_12.04.18\_16.09.42.0.log**

This error occurs when a keystore element exists in the configuration without an ID field. If you use a minimal SSL configuration, set the ID field to defaultKeyStore.

**You might get an exception if using a LDAP user registry with sslEnabled and a sslRef value is not specified.**

For example, a configuration has sslEnabled set to true but there is not a sslRef value, as shown in the following example:

```
<ldapRegistry id="ldap" realm="SampleLdapIDSRealm"  
host="ccwin12.austin.ibm.com" port="636" ignoreCase="true"  
baseDN="o=ibm,c=us"  
bindDN="cn=root"
```

```
bindPassword="rootpwd"
ldapType="IBM Tivoli Directory Server"
idsFilters="ibm_dir_server"
sslEnabled="true"
searchTimeout="8m" />
```

You must enter a `sslRef` value. If you are using a minimal SSL configuration that is similar to the following:

```
<ltkeyStore id="defaultKeyStore" location="key.jks"
password="mypassword" />
```

the `sslRef` field should be set to `defaultSSLConfig`.

If a custom SSL configuration is configured, the name of that configuration should be placed in the `sslRef` field.

### If you use a JDK from the WebSphere Application Server, you might see the following error if SSL is enabled on your Liberty Server.

```
java.net.SocketException: java.lang.ClassNotFoundException: Cannot find the specified class com.ibm.websphere.ssl.protocol.SSLSocketFactory
    at javax.net.ssl.DefaultSSLContextImpl.createSocket(SSLContextImpl.java:11)
    at javax.net.ssl.DefaultSSLContextImpl.createSocket(SSLContextImpl.java:6)
    at com.ibm.net.ssl.www2.protocol.https.c.afterConnect(c.java:161)
    at com.ibm.net.ssl.www2.protocol.https.d.connect(d.java:36)
    at sun.net.www.protocol.http.HttpURLConnection.getInputStream(HttpURLConnection.java:1184)
    at java.net.HttpURLConnection.getResponseCode(HttpURLConnection.java:390)
    at com.ibm.net.ssl.www2.protocol.https.b.getResponseCode(b.java:75)
    at com.ibm.ws.jmx.connector.client.rest.internal.RESTBeanServerConnection.loadJMXServerInfo(RESTBeanServerConnection.java:114)
    at com.ibm.ws.jmx.connector.client.rest.internal.RESTBeanServerConnection.<init>(RESTBeanServerConnection.java:114)
    at com.ibm.ws.jmx.connector.client.rest.internal.Connector.connect(Connector.java:315)
    at com.ibm.ws.jmx.connector.client.rest.internal.Connector.connect(Connector.java:103)
```

This error occurs because the WebSphere Application Server SSL socket factories are not supported by Liberty. You can get past this problem by taking the following steps:

- Create a text file, such as `my.java.security` with the following two empty entries
 

```
ssl.SocketFactory.provider=
ssl.ServerSocketFactory.provider=
```
- Create a `jvm.options` file for your Liberty server
- Add the following property to your `jvm.options` file, that includes the full path to your text file that you just created
 

```
-Djava.security.properties=fullPathTo/my.java.security
```
- If you want to make this more reusable, you can put the `my.java.security` file in your server directory, and then you will be able to use a relative path like this:
 

```
-Djava.security.properties=./my.java.security
```

For more information, see “Customizing the Liberty environment” on page 1565.

## Troubleshooting CORBA/IIOP

This section describes some common CORBA problems and solutions you can choose.

### If you use a JDK from the WebSphere Application Server, you might see the following error if your application uses CORBA/IIOP communications.

```
15:21:58.096 com.ibm.rmi.pi.InterceptorManager runPreInit:178 Init Process ORBRas [default] java.lang.ClassNotFoundException: com.ibm.ISecurityLocalObjectBaseL13Impl.CSIClientRI
    at com.ibm.CORBA.iiop.UtilDelegateImpl.loadClass(UtilDelegateImpl.java:685)
    at javax.rmi.CORBA.Util.loadClass(Util.java:246)
    at com.ibm.rmi.pi.InterceptorManager.runPreInit(InterceptorManager.java:172)
    at com.ibm.rmi.corba.ORB.initializeInterceptors(ORB.java:664)
    at com.ibm.CORBA.iiop.ORB.initializeInterceptors(ORB.java:1084)
    at com.ibm.rmi.corba.ORB.orbParameters(ORB.java:1359)
```

```

at com.ibm.rmi.corba.ORB.set_parameters(ORB.java:1271)
at com.ibm.CORBA.iiop.ORB.set_parameters(ORB.java:1694)
at org.omg.CORBA.ORB.init(ORB.java:371)
...

```

This error occurs because the WebSphere Application Server Object Request Broker (ORB) interceptors are not supported by Liberty. You can resolve this problem by editing the orb.properties file from the JDK to not use these interceptors. This file is usually found in the WebSphere <JAVA\_HOME>/jre/lib directory directory, though you might have overridden it with a copy in the user's <USER\_HOME> directory. The following example shows the lines in the orb.properties file that must be commented out:

```

# WS Interceptors
#org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.ws.Transaction.JTS.TxInterceptorInitializer
#org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.ejs.ras.RasContextSupport
#org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.ISecurityLocalObjectBaseL13Impl.ClientRIWrapper
#org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.ws.activity.remote.cos.ActivityServiceClientInterceptor
#org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.ISecurityLocalObjectBaseL13Impl.CSIClientRI
#org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.debug.olt.ivbtrjrt.OLT_RI
#org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.ws.wlm.client.WLMClientInitializer

# WS ORB & Plugins properties
#com.ibm.ws.orb.transport.ConnectionInterceptorName=com.ibm.ISecurityLocalObjectBaseL13Impl.SecurityConnectionInter

```

## Troubleshooting logging and tracing

This section describes some common problems with logging and tracing.

### The java.util.logging -- Java logging programming interface.

Liberty does not support using the logging.properties file to configure java.util.logging. Use java code, for example in a deployed application or user feature, to create and add java.util.logging handlers, filters, or formatters.

Since the Liberty server manages the java.util.logging logger levels in accordance with the traceSpecification attribute of the logging configuration element, you should avoid using the Logger.setLevel method.

## Troubleshooting JAX-WS

This section describes some common JAX-WS problems and solutions you can choose.

### The org.apache.cxf.bus.extension.ExtensionException occurred when deploying web services application on Liberty.

If your application has CXF libraries and configurations embedded already and you want to deploy the application to Liberty, you must make sure that the jaxws-2.2 server feature is disabled by removing the feature from the server.xml file.

### The java.lang.NoClassDefFoundError exception occurred when running IBM fastpath with the Oracle JVM.

To use IBM fastpath Java Architecture for XML Binding (JAXB), you can configure the com.ibm.xml.xlsp.jaxb.opti.level custom property to control whether optimization methods are enabled for JAXB unmarshalling (deserialization) and marshalling (serialization). If you are experiencing the java.lang.NoClassDefFoundError exception when running IBM fastpath JAXB with the Oracle JVM, you can change the value of com.ibm.xml.xlsp.jaxb.opti.level property to 0 to turn off the optimization. For example, you can use the -Dcom.ibm.xml.xlsp.jaxb.opti.level=0 property in the command line, or add the following line to the jvm.options file:

```

# Turn off the JAXB optimization
-Dcom.ibm.xml.xlsp.jaxb.opti.level=0

```

See more information of the com.ibm.xml.xlsp.jaxb.opti.level property on the Java virtual machine custom properties page.

**The java.lang.NoClassDefFoundError : com.ibm.CORBA.iiop.ORB exception occurred when running the WebSphere Application Server traditional thin client with the Oracle JVM.**

This error occurs when you try to run the WebSphere Application Server traditional thin client with the Oracle JVM and the jaxws-2.2 feature is already enabled on Liberty. To resolve this problem, you can use the `-Dcom.ibm.websphere.thinclient=true` property when running the WebSphere Application Server traditional thin client as follows:

```
java -Dcom.ibm.websphere.thinclient=true
-cp <classpath_entries_including_classic_thinclient_jar> <WebServicesClientEntryClass> <any_more_parameters>
```

See the similar information of the `com.ibm.websphere.thinclient` property on the PM39777: ADMINISTRATIVE THIN CLIENT USING SOAP CONNECTOR AND SUN JDK DOES NOT WORK page.

**An Empty file returned when retrieving binary files from an MTOM service to a MTOM client.**

This scenario happens when a MTOM client sent binary files successfully to an MTOM service, but an empty file is returned when retrieving the same binary files back from the MTOM service.

As a workaround, you can create a new `DataHandler` and initialize the `DataHandler` by filling the content of the binary file. For example, use a `FileDataSource` object to read from I/O and return the newly created `DataHandler` back , and then pass the `DataHandler` to other web services.

```
...
File f = new File("received_image");
if (f.exists()) {
    f.delete();
}

FileOutputStream fos = new FileOutputStream(f);
img_in.writeTo(fos);

FileDataSource fos_out = new FileDataSource(f);
DataHandler img_out = new DataHandler(fos_out);
return img_out;
...
```

**The javax.xml.ws.soap.SOAPFaultException: Unmarshalling Error occurred when using XMLGregorianCalendar in xsd:gMonth format with the Oracle JVM.**

This error occurs when you use the `XMLGregorianCalendar` class to store `gMonth` format constants as part of your SOAP request on client side and the jaxws-2.2 feature is enabled on Liberty with the Oracle JVM. The root cause is that the Oracle JVM supports the new standard format `--MM` for the `xsd:gMonth` type while the latest JAXB RI (Reference Implementation) only supports the format of `--MM--`.

To resolve this problem, you can change the Oracle JVM to the IBM JVM for both the client side and the server side applications.

**The java.io.FileNotFoundException occurred when resolving WSDL files specified by the wsdlLocation attribute.**

This error occurs when you specify the WSDL file as in the code `wsdlLocation = "file:/WEB-INF/wsdl/a.wsdl"` and the WSDL file is packaged within your application. If you want to refer to the WSDL file that is packaged in your application, you must use relative URIs for the `wsdlLocation` attribute defined in the `@WebService`, `@WebServiceProvider`, `@WebServiceClient` or `@WebServiceRef` annotation.

The relative URI for the `wsdlLocation` attribute must be one of the following values:

- `wsdlLocation = "/WEB-INF/wsdl/a.wsdl"`
- `wsdlLocation = "WEB-INF/wsdl/a.wsdl"`

**A large number of "Creating service" messages occur in the messages.log file.**

This scenario happens when you call the `getPort` or related methods in the generated client stub

classes. Liberty is configured with the default logging configuration, and all the information messages are written into the messages.log file. There are lots of occurrences of messages that might be similar to the following one:

```
00000037 org.apache.cxf.service.factory.ReflectionServiceFactoryBean I Creating Service {http://www.echo.org/}EchoService from WSDL:
wsjar:file:/wlp/usr/servers/default/workarea/org.eclipse.osgi/bundles/100/data/cache/
com.ibm.ws.app.manager_gen_15a42559-f979-4ee6-b488-9fa1fb212c96/.cache/Echo.war!/WEB-INF/wsdl/Echo.wsdl
```

To suppress these information messages, you can change the logging configuration in the server.xml file as follows:

```
<logging traceSpecification="org.apache.cxf.*=warning=enabled"/>
```

**The SOAPFaultException: The given SOAPAction *test* does not match an operation occurred when a client application sent a SOAP Action.**

**Note:** *test* is the value of the soapAction attribute in the request HTTP header.

Each operation in a SOAP web service can be associated with a SOAP Action String, such as in the WSDL binding or via an annotation. The web service client sends the SOAP Action string as a header with the request to match the operation of the web service provider. The error message is displayed in either of the following scenarios:

- When the SOAP action sent by the client does not match the SOAP action of the operation.
- When using the WebSphere Application Server traditional as the JAX-WS client and Liberty as the JAX-WS service and the soapAction defined in the WSDL file equals empty value "".

To resolve this problem:

- Make sure that you specify the same SOAP action for both the web service client and service provider.
- Provide a valid value to the soapAction attribute that is defined in the WSDL file or do not use soapAction in the WSDL file.

**The javax.xml.ws.WebServiceException occurred when using the Service.create() method to create service.**

This error occurs when you use the Service.create() method to create a service while the WSDL document is not provided. If you want to use the Service.create() to create a service and getPort() method to get the port number, you must use the addPort() method to provide the binding information.

A sample example code is provided as follows on how to use the addPort() method:

```
QName serviceName = new QName("http://test.com/wssvt/acme/InsBusiness/", "MTOM11Service");
QName portName = new QName("http://test.com/wssvt/acme/InsBusiness/", "MTOM11Port");

// Setup the necessary JAX-WS artifacts
Service svc = Service.create(serviceName);
// Add the port in the service instance
svc.addPort(portName, SOAPBinding.SOAP11HTTP_MTOM_BINDING, mtom11URL);

port = svc.getPort(portName, MTOMInterface.class);
```

**The Null Response returned when the name attribute in @WebResult annotation is different from the name element in the WSDL document.**

This problem occurs when you use a SEI class to define the **name** attribute for @WebResult annotation, and the SEI class has supplied WSDL location as follows:

```
@WebService(wsdlLocation="WEB-INF/wsdl/WebServiceIfc.wsdl")
public interface WebServiceRuntimeIfc {
    @WebMethod
    @WebResult(name="nononoreturn")
    public String echo (String parm);
}
```

But the XML element declaration in the supplied WSDL document is as follows:

```

<xs:element name="echoResponse">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="return" type="xs:string" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

Then the web service client will get a NULL response when the echo() method is called.

To resolve this problem, you must make sure that the **name** attribute of @WebResult annotation match the value of name element in the WSDL document.

### The JAX-WS client application failed to get the WSDL document changes from the server side.

The problem occurs when the web service client and service provider are in two different applications on Liberty, and the client needs to retrieve the WSDL document from the service provider dynamically. Because Liberty caches the WSDL definition when the WSDL document is accessed for the first time, which is different from the behavior in the WebSphere Application Server traditional. By caching the WSDL definition in Liberty, applications can avoid connecting and parsing the WSDL document frequently.

To solve this problem, you have to restart the client application so that the updated wsdl definitions can be reloaded.

### WebApp in Liberty hangs if a web service refers to itself.

If you use annotation @WebService for a web service and the annotation @WebServiceRef to refer to itself, the service endpoint publishing fails. For example,

```

@WebService
public class Test {
    @WebServiceRef
    private Test selfservice;

    public String echo(String msg) {
        return selfservice.invoke();
    }

    public String invoke() {
        return "hello world";
    }
}

```

To avoid this issue, use the service-stub (TestService as is shown in the following example) to get the service instance instead of using the @WebServiceRef to refer to self-service. For example,

```

@WebService
public class Test {

    private Test selfservice;

    public String echo(String msg) {
        TestService ts=new TestService();
        selfservice=ts.getTestPort();
        return selfservice.invoke();
    }

    public String invoke() {
        return "hello world";
    }
}

```

### Different behavior of the WebSphere Application Server traditional and Liberty when policies are attached to both of the service level and the operation level

The behaviors of the WebSphere Application Server traditional and Liberty are different when

policies are attached to both of the service level and the operation level. When both policies of service and operation level are applied, as is shown in the following example,

```
<wsdl:binding name="UrnMustUnderstandBinding2" type="tns:MustUnderstand">
  <wsp:PolicyReference URI="#UserNameToken1" />
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <wsdl:operation name="invoke">
    <soap:operation soapAction="" style="document"/>
    <wsdl:input name="getVerRequest">
      <soap:body use="literal"/>
      <wsp:PolicyReference URI="#UserNameToken2" />
    </wsdl:input>
    <wsdl:output name="getVerResponse">
      <soap:body use="literal"/>
    </wsdl:output>
  </wsdl:operation>
</wsdl:binding>
```

- For the WebSphere Application Server traditional, the expected behavior is that if the operation name in SOAP request matches the operation name of <wsdl:input> like "getVerRequest", the policy of operation level "#UserNameToken2" is applied only.
- For Liberty,
  - If some SOAP requests match the expectation of "#UserNameToken2", the "#UserNameToken2" policy is applied.
  - If some SOAP requests do not match the expectation of "#UserNameToken2", the "#UserNameToken1" policy is applied.

If you want the behavior in the Liberty level to be the same as in the WebSphere Application Server traditional, declare the policies that have the same or similar function at one level only, either at the service level or at the operation level.

## Troubleshooting WS-Security

This section describes some common solutions that you can use to solve WS-Security problems.

1. Check the server.xml file to make sure that the required JAX-WS (jaxws-2.2) and security (appSecurity-2.0) features are configured correctly.
2. To protect your web service application with WS-Security, your JAX-WS application must contain a WSDL file that has an embedded WS-Security policy. There must be a PolicyReference to the embedded WS-Security policy in either the wsdl:binding or wsdl:operation sections or both.
3. If you use a callback handler for retrieving passwords to generate UsernameTokens or for retrieving passwords for private keys from keystore files, the password callback handler must be packaged and deployed as a user feature in Liberty.

### Enabling WS-Security trace

If the cause of the problem cannot be determined by the information in the error message, you can use the Liberty trace and logging facility to collect trace for the WS-Security component. See Liberty: Trace and logging.

You can use the following trace string to collect trace to debug WS-Security failures:

```
org.apache.ws.security.*=all=enabled:
org.apache.cxf.ws.security.*=all=enabled:
org.apache.cxf.ws.policy.*=all=enabled
org.apache.xml.security.*=all=enabled:
com.ibm.ws.wssecurity.*=all=enabled
```

This section described some common WS-Security problems and solutions you can choose.

**org.apache.cxf.ws.policy.PolicyException: None of the policy alternatives can be satisfied.**

This error usually occurs when the WS-Security feature wsSecurity-1.1 is not defined in the server.xml file. To avoid this error, you must define the wsSecurity-1.1 feature in the server.xml file as follows:

```
<featureManager>
  <feature>usr:wssecbh-1.0</feature>
  <feature>servlet-3.0</feature>
  <feature>appSecurity-2.0</feature>
  <feature>jaxws-2.2</feature>
  <feature>wsSecurity-1.1</feature>
</featureManager>
```

**org.apache.cxf.ws.policy.PolicyException: No callback handler and no password available.**

This error occurs when the WS-Security run time cannot retrieve a password that is required to generate a UsernameToken or to access a private key from the keystore. To avoid this error, check the following configuration:

1. Ensure that the password callback handler feature wssecbh-1.0 is defined as a user feature in the server.xml file:

```
<featureManager>
  <feature>usr:wssecbh-1.0</feature>
  <feature>servlet-3.0</feature>
  <feature>appSecurity-2.0</feature>
  <feature>jaxws-2.2</feature>
  <feature>wsSecurity-1.1</feature>
</featureManager>
```

2. Ensure that the callback handler property ws-security.callback-handler is defined in the <wsSecurityClient> or <wsSecurityProvider> elements of the server.xml file:

```
ws-security.callback-handler="<full class name of the callback handler>"
```

example:

```
ws-security.callback-handler="com.ibm.ws.wssecurity.example.cbh.CommonPasswordCallback"
```

3. Ensure that the password callback handler returns the correct password for the user name or the key alias that is specified in the server.xml file. The password must be clear text and not encoded or encrypted.

**org.apache.ws.security.WSSecurityException: The signature does not cover the required elements (soap:Body).**

This error occurs when a web service provider application expects the SOAP body in the request message to be signed, but the received SOAP message does not have the SOAP body signed. To avoid this error, ensure that your web service client is configured with the correct WS-Security policy that matches the web service provider policy.

**org.apache.ws.security.WSSecurityException: The signature or decryption was invalid.**

This error occurs when the WS-Security run time fails to validate the signature or decrypt an encrypted message part in the received SOAP message. To avoid this error, verify that the correct keys are used when you configure WS-Security in the <wsSecurityClient> and <wsSecurityProvider> elements of the server.xml file. If a web service client uses Bob's public key to encrypt a message part, then the web service provider must have access to Bob's private key to decrypt the message. Similarly, if a web service client signs a message part by using Alice's private key, then the web service provider must use Alice's public key to validate the signature.

**org.apache.cxf.ws.policy.PolicyException: These policy alternatives can not be satisfied.**

This error occurs when the WS-Security run time cannot process the incoming SOAP message successfully by using the WS-Security policy that is configured to process this request. To avoid this error, look at the messages that follow this exception to determine the specific WS-Security policy assertions that are causing this exception. For example, the log file might contain the following messages:

```
Caused by: org.apache.cxf.ws.policy.PolicyException: These policy alternatives can not be satisfied:
{http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702}AsymmetricBinding: The encryption algorithm does not match the requirement
{http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702}InitiatorEncryptionToken
```

```
{http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702}RecipientEncryptionToken
at org.apache.cxf.ws.policy.AssertionInfoMap.checkEffectivePolicy(AssertionInfoMap.java:167)
at org.apache.cxf.ws.policy.PolicyVerificationInInterceptor.handle(PolicyVerificationInInterceptor.java:101)
```

In this case, the error occurred because the encryption algorithm that is used by the web service client does not match the encryption algorithm that is specified by the AlgorithmSuite assertion. The algorithm suites that are specified in the WS-Security policy of both the web service client and the web service provider must specify the same encryption algorithm.

### **javax.xml.ws.soap.SOAPFaultException: The message has expired (WSSecurityEngine: Invalid timestamp The security semantics of the message have expired).**

This message occurs when the message timestamp is expired or the message was created with a timestamp in the future.

Distributed operating systems

IBM i

## **Applying fix packs and interim fixes to an archive install**

If you installed your Liberty runtime environment from an archive file, rather than by using Installation Manager, you must take special measures when you apply service updates. For more information, see “Applying a fix pack to a Liberty Java archive installation” on page 1380 and “Applying an interim fix to a Liberty archive installation” on page 1388.

## **Troubleshooting performance**

This section describes some common performance problems and solutions you can choose.

### **High CPU usage by your application monitor.**

This error can occur if your application monitor has many files under the apps/ directory and is polling too frequently.

To avoid this problem there are a number of things you can change.

1. Increase the value of the pollingRate attribute.
2. Update the server.xml to include an applicationMonitor element with an updateTrigger that is not polled.

```
server.xml
<applicationMonitor updateTrigger="mbean" />
```

3. Reduce the number of files under the apps/ directory.

For more information about the applicationMonitor element, see “Controlling dynamic updates” on page 1594.

8.5.5.7

## **Troubleshooting SAML**

This section describes some common problems with SAML and the solutions you must apply.

### **java.lang.ArrayIndexOutOfBoundsException: Array index out of range: 0**

This exception can occur when attempting multiple logins through an unsolicited Service Provider (SP) initiated request without removing the Identity Provider token (IdP).

To avoid this, add `<httpSession invalidateOnUnauthorizedSessionRequestException="true" />` in the relevant unsolicited server.xml file.

### **java.lang.IllegalStateException: CWWKS0010E: While getting the caller principal, the caller subject was found to have more than one principal of type WSPincipal. Only one WSPincipal can exist in the subject. The names of the WSPincipals are: {0}**

This exception can occur if a SAML user has previously logged directly into an on-premises user registry. To avoid this problem, a SAML user must not directly login to an on-premises user registry.

---

## Security bulletins for the Liberty profile

To avoid preventable security issues, stay up to date on the most current maintenance options for the product.

### Subscription to security bulletins

Subscribe to My Notifications to receive notifications of security bulletins for WebSphere Application Server. These notifications include important product support alerts.

### Update Strategy

Refer to the Update Strategy for fix packs. Take special note of the recommended update path.

### Security fixes

Refer to the security fixes for WebSphere Application Server traditional, WebSphere Application Server Liberty, IBM HTTP Server, and Java.

---

## Logstash collector

8.5.5.9

Liberty generates various events at runtime, such as log events, trace events, first failure data capture (ffdc) events, access log events, and garbage collection events. It is helpful to consolidate events from all servers so the events can be searched, filtered, and analyzed, particularly when you are managing many servers, or when you are running servers on different platforms (for example on dedicated hardware and in the cloud). It can also be helpful to store events on a separate server in cases where you use Liberty in environments that lack persistent file storage for problem determination data. Liberty now provides the Logstash collector feature to help you remotely consolidate events. You can avoid running the agents on your Liberty server machine to collect your events using this feature. The collector captures in-flight events, breaks them into fields, and securely forwards the events to the configured Logstash server.

### Logstash collector

The Logstash collector feature (logstashCollector-1.0) sends events to a Logstash server that you provide.

The logstash collector feature offers a flexible way to choose one or more of the following supported sources of data that needs to be sent to logstash:

- message - messages log events
- trace - traces log events
- accesslog - Http access log events
- ffdc - FFDC log events
- garbageCollection - GarbageCollection events

Logstash can be used with the Elasticsearch search server and Kibana dashboard, all of which you provide, set up, and manage, to give a consolidated view of logs or other events from across your enterprise. Note that there are no separate processes or agents to be set up on the Liberty server machine when using the Logstash collector to forward events.

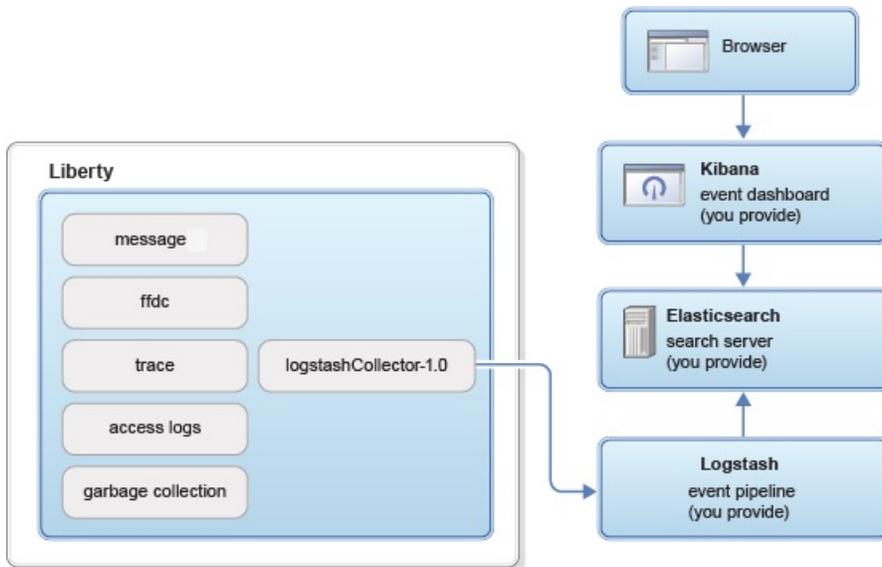


Figure 32. Logstash collector

## Event structure

The collectors send each event as a set of field name-value pairs. Each different type of event has its own set of fields. Knowing which fields each event has is useful when creating your own Kibana dashboards.

The following fields are common and present in all events:

- type – a string that identifies the type of event
- datetime – time at which the event occurred
- hostName – host name of the server that was the source of the event
- wlpUserDir – user directory of the server that was the source of the event, for example, D:\wlp\usr
- serverName – server name of the server that was the source of the event
- sequence – sequence number of event (useful for sorting records with the same time stamp)

Besides the common fields, each of the event types also has its own unique fields:

### Message events (type:"liberty\_message")

- severity – 1 letter severity indicator (F = Fatal, E = Error, W = Warning, A = Audit, I = Info, O = SystemOut, R = SystemErr)
- messageId – message ID in the log line, which can be used to find out specific types of errors, for example, SRVE0250I
- methodName – method name from log record
- className – class name from log record
- loggerName – logger name from log record
- threadId – thread ID in the log line, for example, 00000015. Note that the thread ID is a string and not a number
- message – the message, starting with the message ID

### Trace events (type:"liberty\_trace")

- severity – 1 letter severity indicator (1 = Fine, 2 = Finer, 3 = Finest, > = Entry, < = Exit)

methodName – method name from log record  
className – class name from log record  
loggerName – logger name from log record  
threadId – thread ID in the log line, for example, 00000015. Note that the thread ID is a string and not a number  
message – the message

#### **HTTP access log events (type:"liberty\_accesslog")**

uriPath – Path information for the requested URL. This does NOT contain the query parameters, for example, /pushworksserver/ push/apps/tags  
requestMethod – HTTP verb used, for example, GET  
remoteHost – remote host IP address in the log line, for example, 127.0.0.1  
userAgent – userAgent value in the request.  
requestProtocol – Protocol information in the log line, for example, HTTP/1.1  
queryString – string representing query string from the HTTP request, for example, color=blue&size=large  
bytesReceived – bytes received in the URL, for example, 94 in the sample 1  
responseCode – HTTP response code, for example, 200  
elapsedTime – time that is taken to serve the request  
requestHost – request host IP address in the log line, for example, 127.0.0.1  
requestPort – port number of the request

#### **FFDC events (type:"liberty\_ffdc")**

className – the class that emitted the FFDC entry  
exceptionName – the exception that was reported in the FFDC entry  
probeID – the unique identifier of the FFDC point within the class  
stackTrace – the stack trace of the FFDC incident  
objectDetails – the incident details for the FFDC incident  
threadId – the thread ID of the ffdc incident

#### **Garbage Collection events (type:"liberty\_gc")**

heap – the total heap available  
usedHeap – the amount of heap used  
duration – the duration for which GarbageCollection was run  
gcType – the type of garbage collection event (for example: Nursery, Global, etc.)  
reason – the reason for garbage collection

## **Using the Logstash collector**

8.5.5.9

Use the Logstash collector feature in Liberty to collect log and other events from your Liberty servers and send them to a remote Logstash server. The collected events can be used for log analysis and troubleshooting purposes.

## Before you begin

The logstashCollector-1.0 feature was tested with Logstash V2.x, Elasticsearch V2.x, and Kibana V4.x. You can use the logstashCollector-1.0 feature with a Logstash server that runs with any of the available output plug-ins from Logstash. However, many users choose to use Logstash V2.x with Elasticsearch V2.x and Kibana V4.x to provide a complete log consolidation and analysis facility. For more information, see Elasticsearch.

## Procedure

1. Set up Logstash V2.x by following the instructions from Elasticsearch.
2. Create or acquire certificate and key pair files for SSL for Logstash. The following example is the command for openssl that can be used for generating a certificate and key pair. Customize the number of days the keys are valid as required.

```
openssl req -x509 -newkey rsa:2048 -keyout logstash.key -out logstash.crt -days 365 -nodes
```

3. For Logstash V2.x and Elasticsearch users, copy the sample into a `liberty_logstash_template.json` file. See the repository for a sample Logstash index template. Customize the `_ttl` defaults as required to indicate the number of milliseconds to keep records of each event type.
4. For Logstash V2.x and Elasticsearch users, copy the sample into a `liberty_logstash.conf` file. See the repository for sample Logstash filters. Customize lumberjack `ssl_certificate` path, `ssl_key` path, and port number as required. Customize Elasticsearch hosts and template path as required.
5. Complete the following steps for each of the Liberty servers that you want to collect events from:

- a. Acquire or create a keystore for the Liberty server. To create a self-signed certificate use the following command. Customize the server name, password, and subject as required.

```
d:\wlp\bin\securityUtility createSSLCertificate --server=myServerName --password="Liberty" --subject=CN=myHostname,OU=defaultServer,C
```

- b. Import the `logstash.crt` file from step 2 into your server's `key.jks` file. Customize the `wlp_install_dir` and server name as required. When prompted for a password, use the certificate password from step 5a.

```
d:\java\bin\keytool -import -noprompt -alias logstash -file logstash.crt -keystore wlp_install_dir\usr\servers\myServerName\resources
```

- c. Run the following command to install the logstashcollector-1.0 feature:

```
d:\wlp\bin\installUtility install logstashcollector-1.0
```

- d. Configure Logstash collector in the `server.xml` file in Liberty by adding the following content. Customize the logstashCollector list of sources, host name, and port as required.

```
<featureManager>
  <feature>logstashCollector-1.0</feature>
</featureManager>

<keyStore id="defaultKeyStore" password="Liberty" />

<ssl id="mySSLConfig" trustStoreRef="defaultKeyStore" keyStoreRef="defaultKeyStore" />

<logstashCollector
  source="message,trace,garbageCollection,ffdc,accessLog"
  hostName="localhost"
  port="5043"
  sslRef="mySSLConfig"
/>
```

**Note:** Trace and access logs are usually high volume logs and require more network, CPU, and storage resources to collect.

6. For users of Elasticsearch and Kibana V4.x, import the Kibana dashboard as follows:
  - a. Save the Kibana dashboard JSON to a file on your local file system. For Elasticsearch and Kibana V4.x users, see the repository for a sample Kibana dashboard.
  - b. Import the dashboard into Kibana by clicking **Settings > Objects > Import..** When prompted provide the path to the file you saved in the previous step.

7. Save the dashboard using the save (disk) icon. Enter "Liberty" in the text box that is provided and click the save icon near the text box. The next time that you visit Kibana from any browser you can reload this dashboard using the load icon and clicking **Liberty**.

## Results

Your Liberty servers are configured to send events to your Logstash server, and you can now view your events in the Liberty dashboard using Kibana.

---

## Liberty:Logging and Trace

The product has a unified logging component that handles messages that are written by the product and provides First Failure Data Capture (FFDC) services.

Additionally, the logging component captures messages that are written to `System.out`, `System.err`, `java.util.logging`, and OSGi logging. The logging component unifies the handling of these messages with other messages written by the product. The logging component is not capable of capturing messages that are written directly by the JVM process, such as `-verbose:gc` output.

There are three primary log files for a server:

1. `console.log` - containing the redirected standard output and standard error from the JVM process. This console output is intended for direct human consumption. The console output contains major events and errors if you use the default `consoleLogLevel` configuration. The console output also contains any messages that are written to the `System.out` and `System.err` streams if you use the default `copySystemStreams` configuration. The console output always contains messages that are written directly by the JVM process, such as `-verbose:gc` output. This file is created only if the **server start** command is used, and its location can be altered only by using the `LOG_DIR` environment variable. For more information, see "Administering Liberty from the command line" on page 1567.
2. `messages.log` - containing all messages except trace messages that are written or captured by the logging component. All messages that are written to this file contain additional information such as the message time stamp and the ID of the thread that wrote the message. This file does not contain messages that are written directly by the JVM process.
3. `trace.log` - containing all messages that are written or captured by the product. This file is created only if you enable additional trace. This file does not contain messages that are written directly by the JVM process.

## Logging configuration

The logging component can be controlled through the server configuration. The primary location for the logging configuration is in the `server.xml` file. Occasionally, you might need to configure trace to diagnose a problem that occurs before the `server.xml` file is processed. In this case, the equivalent configuration properties can be specified in the `bootstrap.properties` file. If a configuration property is specified in both the `bootstrap.properties` file and the `server.xml` file, the value in `bootstrap.properties` is used until the `server.xml` file is processed. Then, the value in the `server.xml` file is used. Avoid specifying different values for the same configuration property in both the `bootstrap.properties` and the `server.xml` file.

Table 184. Logging properties for Liberty. Column 1 contains attributes that can be set in the server.xml file. Column 2 contains equivalent properties that can be used in the bootstrap.properties file. Column 3 provides a description of each logging property.

Attribute	Equivalent property	Description
<b>logDirectory</b>	com.ibm.ws.logging.log.directory	This attribute sets the directory for all log files, excluding the console.log file, but including FFDC. By default, <b>logDirectory</b> is set to the LOG_DIR environment variable. The default LOG_DIR environment variable path is <i>WLP_OUTPUT_DIR/serverName/logs</i> . <b>Avoid trouble:</b> Use the LOG_DIR environment variable or com.ibm.ws.logging.log.directory property rather than the <b>logDirectory</b> attribute to configure the directory in which you want all the messages to be written. Otherwise, a few messages are written initially in the logs directory by default, and then the remaining messages are written to the specified directory based on your configuration. The <b>logDirectory</b> attribute might be used to dynamically update the logs to the specified directory while the server is running.
<b>maxFileSize</b>	com.ibm.ws.logging.max.file.size	The maximum size (in MB) that a log file can reach before it is rolled. The Liberty runtime does only size-based log rolling. To disable this attribute, set the value to 0. The maximum file size is approximate. By default, the value is 20. <b>Note:</b> <b>maxFileSize</b> does not apply to the console.log file.
<b>maxFiles</b>	com.ibm.ws.logging.max.files	If an enforced maximum file size exists, this setting is used to determine how many of each of the log files are kept. This setting also applies to the number of exception logs that summarize exceptions that occurred on any particular day. So if this number is 10, you might have 10 message logs, 10 trace logs, and 10 exception summaries in the ffdc/ directory. By default, the value is 2. <b>Note:</b> <b>maxFiles</b> does not apply to the console.log file.
<b>consoleLogLevel</b>	com.ibm.ws.logging.console.log.level	This filter controls the granularity of messages that go to the console.log file. The valid values are INFO, AUDIT, WARNING, ERROR, and OFF. By default, the level is AUDIT. <b>Note:</b> <b>Distributed operating systems</b> Before you change this value, consider the information in section “Unable to interact with the Liberty server after modifying the console log level settings” in the topic “Liberty: Developer Tools known issues and restrictions” on page 2342.
<b>copySystemStreams</b>	com.ibm.ws.logging.copy.system.streams	If true, messages that are written to the System.out and System.err streams are copied to console.log. If false, those messages are written to configured logs such as messages.log or trace.log, but they are not copied to console.log. The default value is true.

Table 184. Logging properties for Liberty (continued). Column 1 contains attributes that can be set in the server.xml file. Column 2 contains equivalent properties that can be used in the bootstrap.properties file. Column 3 provides a description of each logging property.

Attribute	Equivalent property	Description
<b>messageFileName</b>	com.ibm.ws.logging.message.fileName	The message log has a default name of messages.log. This file always exists, and contains INFO and other (AUDIT, WARNING, ERROR, FAILURE) messages in addition to System.out and System.err. This log also contains time stamps and the issuing thread ID. If the log file is rolled over, the names of earlier log files have the format messages_timestamp.log
<b>suppressSensitiveTrace</b>		The server trace can expose sensitive data when it traces untyped data, such as bytes received over a network connection. This attribute, when set to true, prevents potentially sensitive information from being exposed in log and trace files. The default value is false.
<b>traceFileName</b>	com.ibm.ws.logging.trace.fileName	The trace.log file is only created if additional or detailed trace is enabled. <b>stdout</b> is recognized as a special value, and causes trace to be directed to the original standard out stream.
<b>traceSpecification</b>	com.ibm.ws.logging.trace.specification	The trace string is used to selectively enable trace. The default is *=info.
<b>traceFormat</b>	com.ibm.ws.logging.trace.format	This attribute controls the format of the trace log. The default format for Liberty is ENHANCED. You can also use BASIC and ADVANCED formats as in the traditional.
<b>8.5.5.4 hideMessage</b>	com.ibm.ws.logging.hideMessage	You can use the <b>hideMessage</b> attribute to configure the messages that you want to hide from the console.log and message.log files. If the messages are configured to be hidden, then they are redirected to the trace.log file.  <b>Note:</b> <b>Distributed operating systems</b> Before you use this attribute, consider the information that is given under the <i>Unable to recognize the start of the server when the hideMessage attribute is used to suppress the messages</i> section in the “Liberty: Developer Tools known issues and restrictions” on page 2342 topic.

You can set logging properties in the server configuration file by selecting **Logging and Tracing** in the **Server Configuration** view in the developer tools, or by adding a logging element to the server configuration file as follows:

```
<logging traceSpecification="*=audit:com.myco.mypackage.*=finest"/>
```

The format of the log detail level specification is:

```
<component> = <level>
```

where *<component>* is the component for which to set a log detail level, and *<level>* is one of the valid logger levels (off, fatal, severe, warning, audit, info, config, detail, fine, finer, finest, all). Separate multiple log detail level specifications with colons (:).

**Attention:** For a given logger, the level is determined by the most specific trace specification that applies to that logger.

Components correspond to Java packages and classes, or to collections of Java packages. Use an asterisk (\*) as a wildcard to indicate components that include all the classes in all the packages that are contained by the specified component. For example:

- \* Specifies all traceable code that is running in the application server, including the product system code and customer code.

**com.ibm.ws.\***

Specifies all classes with the package name beginning with com.ibm.ws.

**com.ibm.ws.classloader.JarClassLoader**

Specifies the JarClassLoader class only.

Table 185. Valid logging levels. The following table lists the valid levels for application servers at WebSphere Application Server Version 6 and later.

Version 6 and later logging level	Content / Significance
off	Logging is turned off.
fatal	Task cannot continue and component, application, and server cannot function.
severe	Task cannot continue but component, application, and server can still function. This level can also indicate an impending unrecoverable error.
warning	Potential error or impending error. This level can also indicate a progressive failure (for example, the potential leaking of resources).
audit	Significant event that affects server state or resources
info	General information that outlines overall task progress
config	Configuration change or status
detail	General information that details subtask progress
fine	Trace information - General trace + method entry, exit, and return values
finer	Trace information - Detailed trace
finest	Trace information - A more detailed trace that includes all the detail that is needed to debug problems
all	All events are logged. If you create custom levels, <i>all</i> includes those levels, and can provide a more detailed trace than finest.

The console.log file does not have the same level of management as other log files. The only property that you can change is **consoleLogLevel**. If you are concerned about the increasing size of the console.log file, you can disable the console.log file and use the message log file instead. The same data, in a different format, is written to the message log file, and you can control the size and number of message log files by using the **maxFileSize** and **maxFiles** attributes. For example, the following bootstrap.properties file results in an empty console.log file and a maximum of three rolling 1 MB loggingMessages.log files. However, messages from the underlying JVM can still be written to the console.log. Settings in the bootstrap.properties file take effect before the message log file is created, so the message log file is initially created as loggingMessages.log and not the default messages.log.

```
com.ibm.ws.logging.max.file.size=1
com.ibm.ws.logging.max.files=3
com.ibm.ws.logging.console.log.level=OFF
com.ibm.ws.logging.message.file.name=loggingMessages.log
```

The console.log file is reset when the server is restarted.

**Note:** On all platforms, logs are written in the default system encoding.

- **z/OS** On z/OS systems, the console.log file uses the default code page, and all other log files uses IS08859-1 encoding and are tagged as text files with that encoding. If the z/OS UNIX System Services (USS) automatic code page conversion feature is active, you can use standard editors and text utilities to view the log files that are encoded with IS08859-1.
- **Windows** On Windows systems, there are two types of encoding: OEM code page, which is used for console output, and ANSI code page, which is used to read and write files. The console.log file uses the OEM code page, and all other logs use the ANSI code page.
- **Distributed operating systems** On all other platforms, all log files use the default encoding.

**Note:** For general help on understanding message formats, see Message log interpretation.

---

## Viewing trace and message log files by using developer tools

Linux

Windows

8.5.5.7

You can view trace and message log files for either local or remote servers by using WebSphere Developer Tools.

### Before you begin

- To view the trace file, you must enable tracing by specifying the traceformat and tracespecification settings in the server.xml file or the bootstrap.properties file. For more information about enabling tracing, see Liberty: Logging and Trace.
- You can change the default log file names from messages.log and trace.log, and the default directory name from WLP\_OUTPUT\_DIR/serverName/logs by changing any of the configuration files.
  - Configuration files include server.xml, bootstrap.properties, and server.properties.
- Actions for local servers:
  - Ensure that the log file is in the log directory that you specified. Otherwise, the menu actions for the local server are disabled.
  - If you change the bootstrap.properties file or the server.env file, you must restart the server for changes to take effect. Menu actions are temporarily disabled until the server is restarted.
  - If the same configuration setting is specified in more than one configuration file, the setting in the server.xml file overrides the other values.
- Actions for remote servers:
  - Ensure that the server is running. If it is not running, menu actions are not displayed.
  - If you change the default location of a log file, include remote access by adding either a ReadDir or a WriteDir configuration to your server.xml file to indicate the log location. The following example shows how to add remote access.

```
<logging logDirectory="${server.output.dir}/log_a" maxFiles="10" traceFormat="BASIC" traceSpecification="com.i
<remoteFileAccess>
  <writeDir >${wlp.user.dir}</writeDir>
  <writeDir>${server.config.dir}</writeDir>
  <writeDir>${server.output.dir}</writeDir>
  <writeDir>${server.output.dir}/log_a</writeDir>
</remoteFileAccess>
```

### Procedure

1. To view a list of servers, select **Window > Show View > Servers**.
2. Right-click a server.

- To view the trace log file, select **Open Log Files > Trace File** from the menu.
- To view the messages log file, select **Open Log Files > Message Log File** from the menu.

For remote servers, downloading log files can take several seconds depending on the size of the log file.

## Results

The log file that you selected is displayed in the default editor. The following example shows records in a message log file.

```
[3/3/11 23:01:30:147 EST] 0000000f ApplicationMg Z WSVR0221I: Application started: DefaultApplication
```

In this example, *[3/3/11 23:01:30:147 EST]* is the time stamp, *0000000f* is the thread ID, *ApplicationMg* is the logger, *Z* is the level, *WSVR0221I* is the message ID, and *Application started: DefaultApplication* is the message.

---

## Liberty: Timed operations and JDBC calls

### 8.5.5.0

Timed operations generate a logged warning when JDBC calls in the application server are operating more slowly or quickly than expected.

## Overview

When enabled, the timed operation feature tracks the duration of JDBC operations running in the application server. In cases where operations take more or less time to execute than expected, the timed operation feature logs a warning. Periodically, the timed operation feature will create a report, in the application server log, detailing which operations took longest to execute. If you run the server dump command, the timed operation feature will generate a report containing information about all operations it has tracked. You can use the information listed in these reports to decide if anything is running slower or faster than you expect.

Periodically, the system generates a report to the logs that contains the ten longest JDBC timed operations. The frequency and enablement of this report is configurable in the `server.xml` file, with a default of once per day (24 hours).

To enable timed operations, add the `timedOperations-1.0` feature to the `server.xml` file.

You can disable the generation of the report to the logs, or change the frequency of the report, for example to once every 12 hours, using the `timedOperation` element as shown in the following example:

```
<timedOperation enableReport="false" reportFrequency="12" />
```

You can also use the `maxNumberTimedOperations` attribute to log a warning when the total number of timed operations reaches the value specified by this attribute. The number of timed operations is monitored and useful to know since each timed operation is allocated memory from the heap, and if you find that the number of timed operations is excessive, you can disable the timed operations feature. You can use the following example to configure the `maxNumberTimedOperations` attribute:

```
<timedOperation enableReport="false" reportFrequency="12" maxNumberTimedOperations="10000"/>
```

This example results in a warning message in the log as follows when the number of timed operations exceeds 10000:

[4/18/13 23:01:37:316 EDT] 0000002c com.ibm.wsspi.timedoperations.TimedOperationService W TRAS0094I: The total number of timed operations is 10000, which exceeds the configured maximum number of 10000. You can also find the number of timed operations in the report that is periodically generated to the logs. If you find that the number of timed operations is excessive, you can disable the timed operations feature.

### 8.5.5.2

If you set the value of the *com.ibm.timedOperations.autoCleanup* WebSphere environment variable to true, the server automatically limits the number of tracked timed operations to the value specified in the <maxNumberTimedOperations> attribute. A warning is logged when the total number of timed operations reaches the maximum value specified. To limit the number of tracked timed operations, when a new timed operation is required to be tracked, the least recently used timed operation record is deleted. When the number of timed operations that are tracked reaches the specified maximum value, a warning message is displayed as follows:

TRAS0095I: The total number of timed operations has reached the configured maximum of 10000. As new timed operations are

You can also use the **server dump** command to get a full report of all timed operations in the `messages.log` file, grouped by type, and sorted within each group by average of actual duration.

The following example shows a sample logged message:

```
[3/14/13 14:01:25:960 CDT] 00000025 TimedOperatio W TRAS0080W: Operation websphere.datasourc.execute:
jdbc/exampleDS:insert into cities values ('myHomeCity', 106769, 'myHomeCountry') took 1.541 ms to complete,
which was longer than the expected duration of 0.213 ms based on past observations.
```

The following example shows a sample automatically generated report in the log:

```
[12/13/12 7:42:29:509 CST] 0000001d com.ibm.wsspi.timedoperations.TimedOperationService I TRAS0092I:
The following operations took the longest time to run since the last report has been generated:
Operation websphere.datasourc.execute:jdbc/exampleDS:insert into cities values ('myHomeCity',
106769, 'myHomeCountry') took 194ms to complete
Operation websphere.datasourc.execute:jdbc/exampleDS:select county from cities where name=
'myHomeCity' took 187ms to complete
Operation websphere.datasourc.execute:jdbc/exampleDS:drop table cities took 182ms to
complete\Operation websphere.datasourc.execute:jdbc/exampleDS:insert into cities values
('myHomeCity', 106769, 'myHomeCountry') took 151ms to complete
```

For the full timed operation configuration reference, see the `timedOperation` element in the following topic:

---

## Event Logging



### 8.5.5.6

As part of the monitoring and diagnostic capabilities, the WebSphere Application Server Liberty generates events at various components of Java Platform, Enterprise Edition to track the requests. The `eventLogging-1.0` feature logs such events when the application requests are running. Using this feature, the user can track the requests that are running in the WebSphere Application Server Liberty. Each request is associated with a unique correlator called the request ID and the context information that helps the user to understand the request-specific data.

The event logging feature is controlled through the server configuration. The feature is configured in the `server.xml` file.

The following sample log shows the end-to-end event logs for the `AAY6Ta1VDTO_AAAAAAAAAAAK` request ID and `TradeWeb` context:

```
[12/15/14 18:24:29:528 IST] 0000002e EventLogging I BEGIN requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=webspher
[12/15/14 18:24:29:531 IST] 0000002e EventLogging I BEGIN requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=webspher
[12/15/14 18:24:29:532 IST] 0000002e EventLogging I BEGIN requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=webspher
[12/15/14 18:24:29:533 IST] 0000002e EventLogging I BEGIN requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=webspher
[12/15/14 18:24:29:534 IST] 0000002e EventLogging I BEGIN requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=webspher
[12/15/14 18:24:29:547 IST] 0000002e EventLogging I END requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=websphere.
[12/15/14 18:24:29:556 IST] 0000002e EventLogging I END requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=websphere.
```

```

[12/15/14 18:24:29:671 IST] 0000002e EventLogging I BEGIN requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=websphere.
[12/15/14 18:24:29:672 IST] 0000002e EventLogging I BEGIN requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=websphere.
[12/15/14 18:24:29:677 IST] 0000002e EventLogging I END requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=websphere.da
[12/15/14 18:24:29:684 IST] 0000002e EventLogging I END requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=websphere.se
[12/15/14 18:24:29:685 IST] 0000002e EventLogging I END requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=websphere.se
[12/15/14 18:24:29:686 IST] 0000002e EventLogging I END requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=websphere.se
[12/15/14 18:24:29:687 IST] 0000002e EventLogging I END requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=websphere.se

```

The request begins at the BEGIN websphere.servlet.service "contextInfo=TradeWeb | TradeScenarioServlet" event (refer to the first line in the sample code) and ends at END websphere.servlet.service "contextInfo=TradeWeb | TradeScenarioServlet" (refer to the last line in the sample code). The total time that is taken by this request is also displayed at the end (which is 158.283 ms in the sample code).

You can look at the child requests by looking at the BEGIN and END of the main request. You can also find the time that is taken by each of the child request.

For best performance, you might use binary logging when event logging is enabled. The eventType, contextInfo, and requestID attributes from the event log entries are stored as log record extensions. You can use those log record extensions to filter the logs with the **binaryLog** command.

## Parsing the event log entries in the messages.log file

The event logs capture the information of the events in the following format:

```
[Log mode] [Request Identifier] # [Event Type] # [Context Information] # [Duration] (optional)
```

where

- Log mode indicates whether the log was recorded at the entry to the event or the exit from the event. BEGIN refers to the entry and END refers to the exit.
- Request identifier is a unique string that is assigned to each request. This can be used for filtering events that belong to a specific request.
- Event type provides information about the event source and can be any of the supported event types as given in Table 186.
- Context information of the event provides details relevant to the event type. The information varies depending on the event type.
- Duration indicates the time that is taken by the event. The duration appears only in the exit event entries. Example: 158.283 ms.

Except the log mode, which is separated by a space, all other log attributes are separated by #(space#space). For example,

```
[12/15/14 18:24:29:687 IST] 0000002e EventLogging I END requestID=AAY6Ta1VDTO_AAAAAAAAAAAK # eventType=websphere.servlet.service
```

The following table lists the event types that are supported by event logging:

Table 186. Supported event types along with the relevant context information

Component	Event types	Context information	Example
Servlet	websphere.servlet.destroy websphere.servlet.service	[Application Name]   [Servlet Name]	contextInfo=TradeWeb   display=0   queryString=
Session	websphere.session.dbSessionDestroyed websphere.session.dbSessionDestroyed websphere.session.sessionAccessed websphere.session.sessionCreated websphere.session.sessionDestroyedByTimeout websphere.session.sessionDestroyed websphere.session.sessionLiveCountDec websphere.session.sessionLiveCountInc websphere.session.sessionReleased  websphere.session.getAttribute websphere.session.setAttribute	[Session ID]   [Session Attribute Name]   [Session Attribute Value]	contextInfo=EuitabHZU0D7J2u01HDdAG0   user=

Table 186. Supported event types along with the relevant context information (continued)

Component	Event types	Context information	Example
JDBC	websphere.datasources.execute websphere.datasources.executeQuery websphere.datasources.executeUpdate websphere.datasources.psExecute websphere.datasources.psExecuteQuery websphere.datasources.psExecuteUpdate websphere.datasources.rsCancelRowUpdates websphere.datasources.rsDeleteRow websphere.datasources.rsInsertRow websphere.datasources.rsUpdateRow	Indi Name Of Data Source   conf {SQL in jdbc/TradeDataSource   sele	

## Slow and hung request detection



8.5.5.6

The requestTiming-1.0 feature provides diagnostic information when the duration of any request exceeds the configured threshold.

The request timing feature can track the duration of every request that is coming into the system. You can configure the feature to watch for slow and hung requests.

- “Slow request detection”
- “Hung request detection” on page 2322

### Slow request detection

When a request has been running for longer than configured, a warning message is written in the messages log file. Details about the request and events that made up the request are captured.

The following sample shows the log message for a request that crossed the slow request threshold (default is 10 seconds):

```
[12/1/14 11:58:09:629 IST] 0000001d com.ibm.ws.request.timing.SlowRequestTimer W TRAS0112W: Req

    at java.util.HashMap.getEntry(HashMap.java:516)
    at java.util.HashMap.get(HashMap.java:504)
    at org.apache.derby.iapi.store.access.BackingStoreHashtable.get(Unknown Source)
    at org.apache.derby.impl.sql.execute.HashScanResultSet.getNextRowCore(Unknown Source)
    at org.apache.derby.impl.sql.execute.NestedLoopJoinResultSet.getNextRowCore(Unknown Source)
    at org.apache.derby.impl.sql.execute.ProjectRestrictResultSet.getNextRowCore(Unknown Source)
    at org.apache.derby.impl.sql.execute.DMLWriteResultSet.getNextRowCore(Unknown Source)
    at org.apache.derby.impl.sql.execute.DeleteResultSet.setup(Unknown Source)
    at org.apache.derby.impl.sql.execute.DeleteResultSet.open(Unknown Source)
    at org.apache.derby.impl.sql.GenericPreparedStatement.executeStmt(Unknown Source)
    at org.apache.derby.impl.sql.GenericPreparedStatement.execute(Unknown Source)
    at org.apache.derby.impl.jdbc.EmbedStatement.executeStatement(Unknown Source)
    at org.apache.derby.impl.jdbc.EmbedPreparedStatement.executeStatement(Unknown Source)
    at org.apache.derby.impl.jdbc.EmbedPreparedStatement.executeUpdate(Unknown Source)
    at com.ibm.ws.rsadapter.jdbc.WSJdbcPreparedStatement.executeUpdate(WSJdbcPreparedStatement.java:626)
    at com.ibm.websphere.samples.trade.direct.TradeDirect.resetTrade(TradeDirect.java:1832)
    at com.ibm.websphere.samples.trade.web.TradeConfigServlet.doResetTrade(TradeConfigServlet.java:65)
    at com.ibm.websphere.samples.trade.web.TradeConfigServlet.service(TradeConfigServlet.java:348)
    at javax.servlet.http.HttpServlet.service(HttpServlet.java:668)
    at com.ibm.ws.webcontainer.servlet.ServletWrapper.service(ServletWrapper.java:1275)
    ....
    at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1121)
```

```

at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:614)
at java.lang.Thread.run(Thread.java:769)

```

Duration	Operation
10007.571ms +	websphere.servlet.service   TradeWeb   TradeConfigServlet?action=resetTrade
3.923ms	websphere.datasource.psExecuteUpdate   jdbc/TradeDataSource   delete from holdingejb where holding_
0.853ms	websphere.datasource.psExecuteUpdate   jdbc/TradeDataSource   delete from accountprofileejb where
5271.341ms +	websphere.datasource.psExecuteUpdate   jdbc/TradeDataSource   delete from orderejb where account_

The request continues to be monitored, and a further warning is logged if the request is running beyond another 10 seconds. The log messages are in the following format:

```

TRAS0112W: Request <(Request ID)> has been running on thread <THREADID> for at least <DURATION>. The following stack
<STACK TRACE>
<DURATION AND OPERATIONS Table>

```

### REQUEST ID

This same ID can be used to search for log and trace messages corresponding to the request. In particular, if you use binary logging, you can search for log and trace entries with the same requestID extension by using the binary log command.

### STACK TRACE

Indicates the method that is running. In the previous sample, you can see a stack trace of the current request after TRAS0112W line.

### DURATION AND OPERATIONS Table

After the stack trace, you can find the tabular format of the request that shows the duration and operation (also referred to as the event). The Duration column indicates the time that is taken by the corresponding operation of the request. The plus sign (+) indicates events within the request that are still running. The next line shows the duration without +, which indicates that the corresponding operation has completed in the specified duration. Operation shows the EVENT TYPE and CONTEXT INFO (which is optional) for that operation. For more information about event types and context information, see “Event Logging” on page 2319.

By analyzing the messages, you can figure out why the request is slow. However, it might be difficult to determine whether the request is stuck at that point or is still running slowly. Hence you can see three messages that are logged for any slow request at the interval of specified *<slowRequestThreshold>*. Using the three different stack trace and request data, you get a better insight into the issue. After the third warning, no further warnings are logged about the request unless the duration of the request crosses the hung request detection threshold.

## Hung request detection

If the request exceeds the default hungRequestThreshold or the configured threshold value, a warning message is written in the messages log file along with the details about the request. Details about the request and events that made up the request are captured. In case of hung request detection, a series of three thread dumps (javacores) is taken, with 1 minute delay between them. The following log message sample shows the log messages for a request that crossed the hung request detection threshold. The default duration value is 10 min. The value that is configured in the following example is 4 min.

```

[WARNING ] TRAS0114W: Request AAA7WlpP7I7_AAAAAAAAAAAAA has been running on thread
00000021 for at least 240001.015ms. The following table shows the events that have run during this
request.

```

Duration	Operation
240001.754ms +	websphere.servlet.service   TestWebApp   TestServlet?sleepTime=480000
0.095ms	websphere.session.setAttribute   mCzBMyzMvAEnjMJjx9zQYIw   userID
0.007ms	websphere.session.setAttribute   mCzBMyzMvAEnjMJjx9zQYIw   visitCount

If a request gets completed later, which was detected to be hanging initially, a message similar to the following example is logged: TRAS0115W: Request AAA7WlpP7I7\_AAAAAAAAAAAAA, which was previously detected to be hung, has completed after 479999.681 s.

**Note:** When a request is detected to be hanging, a series of three thread dumps is initiated. After the completion of the three thread dumps, further thread dumps are created only if the new requests are detected to be hanging.

---

## Liberty:Binary logging

8.5.5.0

Binary logging is a high performance log and trace facility based on the High Performance Extensible Logging (HPEL) technology in WebSphere Application Server traditional.

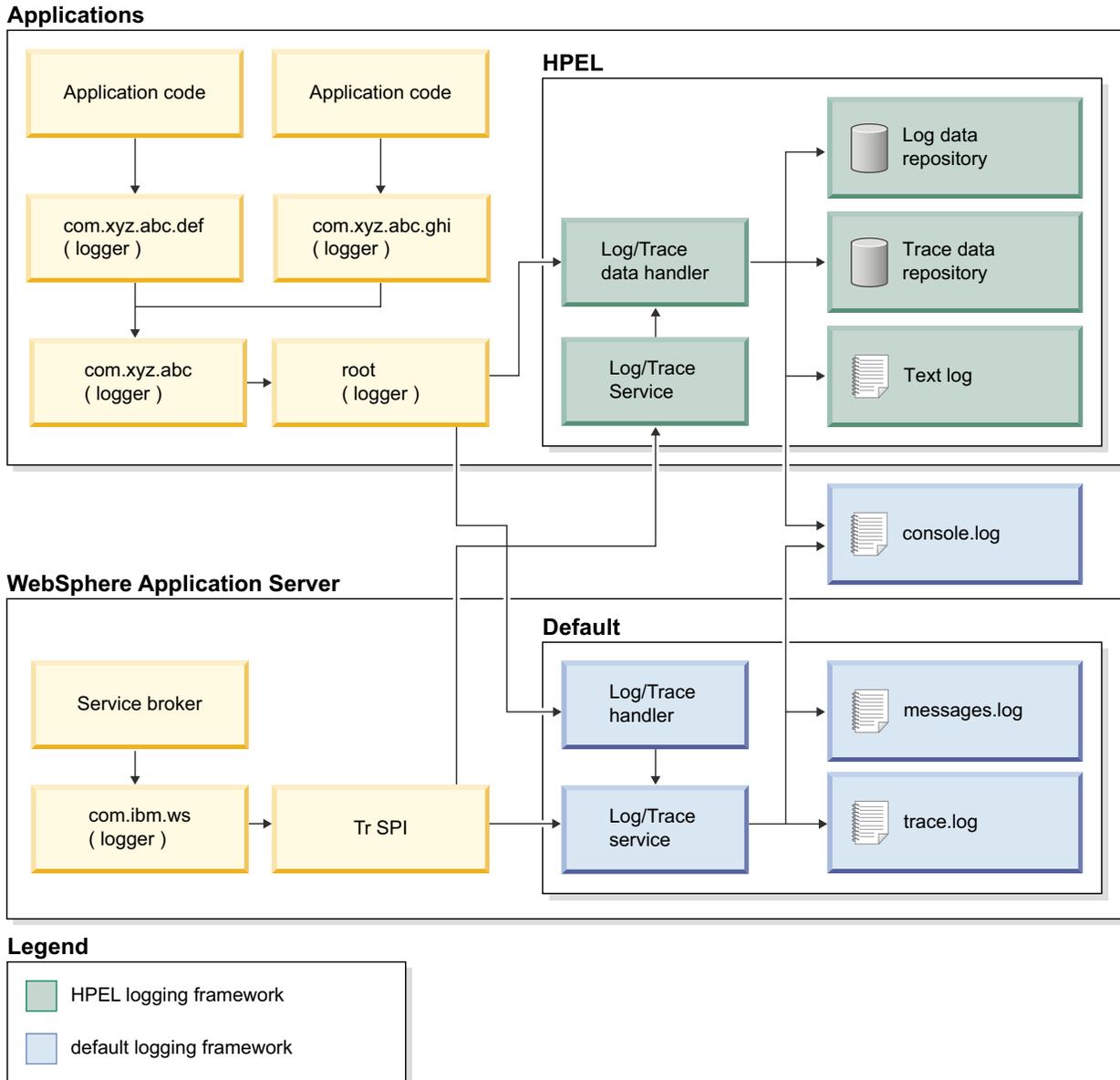
### Overview

**Note:** You must enable the binary logging facility to use it.

Binary logging provides a convenient mechanism for storing and accessing log, trace, System.err, and System.out information produced by the application JVM server or your applications. It is an alternative to the default log and trace facility, which provides the JVM logs and diagnostic trace files commonly named messages.log and trace.log.

### Log and trace storage

Binary logging provides a log data repository and a trace data repository. See the following figure to understand how applications and the application server store log and trace information.



### Log data repository

The log data repository is a storage facility for log records. Log data is typically intended to be reviewed by administrators. This includes any information applications or the server write to System.out, System.err, OSGi logging service at level LOG\_INFO or higher (including LOG\_INFO, LOG\_WARNING, and LOG\_ERROR), or java.util.logging at level Detail or higher (including Detail, Config, Info, Audit, Warning, Severe, Fatal, and any custom levels at level Detail or higher).

### Trace data repository

The trace data repository is a storage facility for trace records. Trace data is typically intended for use by application programmers or by the WebSphere Application Server support team. This includes any information applications or the server write to the OSGi logging service at level LOG\_DEBUG or java.util.logging at levels below level Detail (including Fine, Finer, Finest, and any custom levels below level Detail).

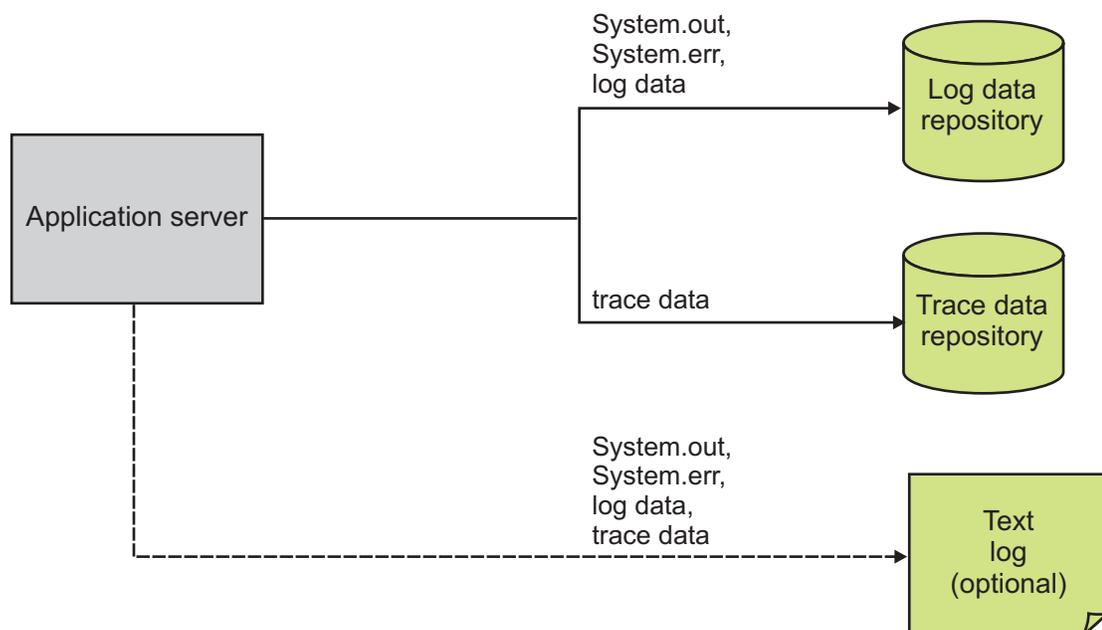
## Log and trace performance

Binary logging has been designed and tested to significantly outperform the default log and trace facility. One result is that the application server can run with trace enabled while causing less impact to performance than tracing the same components using the default log and trace framework. Another result is that applications that frequently write to the logs can run faster when using binary logging.

### Log and trace events are each stored in only one place

Log events, System.out, and System.err are stored in the log data repository. Trace events are stored in the trace data repository. Storing each type of event in only one place ensures that performance is not wasted on redundant data storage.

**Note:** The console log should be disabled in cases where logging performance is important. Any content written to the console log will already be stored in the log data repository.



### Data is not formatted unless it is needed

Formatting data for a user to read uses processor time. Rather than format log event and trace event data at run time, log and trace data are stored more rapidly in a proprietary binary representation. This improves the performance of the log and trace facility. By deferring log and trace formatting until the binaryLog command is run, sections of the log or trace that are never viewed are never formatted.

### Log and trace data are buffered before being written to disk

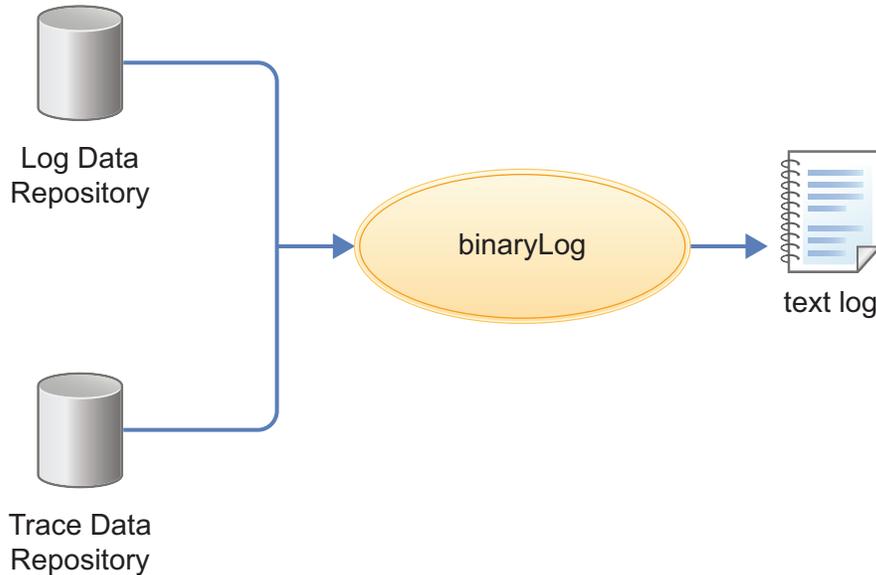
Writing large blocks of data to a disk is more efficient than writing the same amount of data in small blocks. The binary logging facility provides the capability to buffer log and trace data before writing it to disk. By default, log and trace data are stored in an 8 KB buffer before being written to disk. If the buffer is filled within 10 seconds, the buffer is written to disk. If the buffer is not filled within that time it is automatically written to disk to ensure that the logs have the most current information.

## Administration of log and trace

Binary logging has been designed to be easy to configure and understand. For example, administrators can easily configure how much disk space to dedicate to logs or trace, or how long to retain log and trace records, and leave the management of log and trace content up to the server. As another example all log, trace, System.out, and System.err content can be accessed using one easy-to-use command (`binaryLog`), avoiding any possible confusion over which file to access for certain content.

### Reading from the log data and trace data repositories

The log data and trace data repositories are stored in a WebSphere Application Server proprietary format and cannot be read using text file editors such as Notepad or VI. You can copy the log data and trace data repositories in to a plain text format using the `binaryLog` command.



### binaryLog command

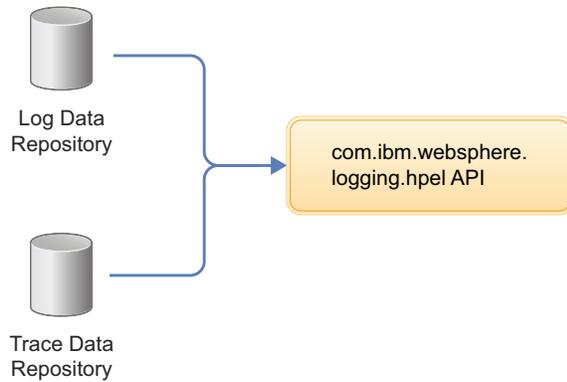
`binaryLog` is an easy-to-use command-line tool provided for users to work with the log data and trace data repositories. `binaryLog` provides filtering and formatting options that make finding important content in the log data and trace data repositories easy. For example, a user might filter any errors or warnings, then filter all log and trace entries that occurred within 10 seconds of a key error message on the same thread.

### Filtering using log and trace record extension content

The binary logging facility provides the capability for developers to add custom extensions to log and trace records using a log record context API (`com.ibm.websphere.logging.hpel.LogRecordContext`). You can use the `binaryLog` command-line tool to filter records based on the content of log and trace record extensions.

## Development resources

Binary logging has been designed to make working with log and trace content more flexible and effective than the default logging facility. Log and trace content can be easily filtered to show only the records that are of interest. You can use the command line (see the description of the `binaryLog` command), or developers can create powerful log handling programs using the HPEL API.



### Reading the log data and trace data

An API has been provided to make it easy for developers to develop tools to consume content from the binary log and trace repositories. For example, a developer might write a Java program to search the log and trace content to find any messages with message IDs that match a known list of important message IDs. This API is in the `com.ibm.websphere.logging.hpel` package. Refer to the API documentation for details on the HPEL log reading API.

### Log and trace record extensibility

Developers can add custom extensions to log and trace records through a log record context API (`com.ibm.websphere.logging.hpel.LogRecordContext`). When binary logging stores log and trace records, it includes any extensions present in the log record context on the same thread. For example, a developer might write a servlet filter to add important HTTP request parameters to the log record context. While that servlet runs, HPEL API adds those extensions to any log and trace records created on the same thread.

As with other log and trace record fields, developers can access the record extensions using the HPEL API. This is useful when writing tools to read from log and trace repositories. Developers can also make use of the log record context API to access extensions in custom log handlers, filters, and formatters at run time.

## BinaryLog command options

8.5.5.0

Use the **binaryLog** command to view or copy the contents of a binary logging repository, or list the available server process instances in the repository. The **binaryLog** command is equivalent to the **logViewer** command in the profile bin directory of the traditional application server.

The binary log and trace facility writes to a repository in a binary format. You can view, query and filter the repository using the **binaryLog** command. The **binaryLog** command provides options for quickly converting repository contents into a text file in various formats, such as basic and advanced formats. The command also provides options to make getting the data you need from the logs easier; for example, allowing you to filter what log records you want by level, logger name, or date and time.

### Syntax

The command syntax is as follows:

```
binaryLog action {serverName | repositoryPath} [options]
```

The value of **options** is different based on the value of **action**.

## Parameters

The following actions are available for the binaryLog command:

### view

Read a repository, optionally filter it, and create a version that users can read.

The command syntax is as follows:

```
binaryLog view {serverName | repositoryPath} [options]
```

*serverName*

Specify the name of a Liberty server with a repository to read from.

*repositoryPath*

Specify the path to a repository to read from. This is typically the directory that contains both the logdata and tracedata directories.

**Note:** If neither a *serverName* nor a *repositoryPath* is specified on the command line, the task is performed against the default server instance, `defaultServer`, if it exists.

Filter options:

All filters are optional. When multiple filters are used, they are logically ANDed together.

- `--minDate=value`  
Filter based on minimum record creation date. Value must be specified as either a date (for example `--minDate="2/20/13"`) or a date and time (for example `--minDate="2/20/13 16:47:21:445 EST"`).
- `--maxDate=value`  
Filter based on maximum record creation date. Value must be specified as either a date (for example `--maxDate="2/20/13"`) or a date and time (for example `--maxDate="2/20/13 16:47:21:445 EST"`).
- `--minLevel=value`  
Filter based on minimum level. Value must be one of FINEST | FINER | FINE | DETAIL | CONFIG | INFO | AUDIT | WARNING | SEVERE | FATAL.
- `--maxLevel=value`  
Filter based on maximum level. Value must be one of the following: FINEST | FINER | FINE | DETAIL | CONFIG | INFO | AUDIT | WARNING | SEVERE | FATAL.
- `--includeLogger=value[,value]*`  
Include records with specified logger name. Value may include \* or ? as a wildcard.
- `--includeMessage=value`  
Filter based on message name. Value may include \* or ? as a wildcard.
- `--includeThread=value`  
Include records with specified thread id. Values must be in hexadecimal (for example, `--includeThread=2a`).
- `--includeExtension=name=value[,name=value]*`  
Include records with specified extension name and value. Value may include \* or ? as a wildcard. To include a comma in the value, you must use "\",
- `--includeInstance=value`  
Include records from the specified server instance. Value must either be "latest" or be a valid instance ID. Run this command using the `listInstances` action to see a list of valid instance IDs.

Monitor option:

`--monitor`

Continuously monitor the repository and output new content as it is generated.

Output options:

- `--format={basic | advanced | CBE-1.0.1}`  
Specify the output format to use. "basic" is the default format.
- `--encoding=value`  
Specify the character encoding to use for output.

## copy

Read a repository, optionally filter it, and write the contents to a new repository.

The command syntax is as follows:

```
binaryLog copy {serverName | repositoryPath} targetPath [options]
```

*serverName*

Specify the name of a Liberty server with a repository to read from.

*repositoryPath*

Specify the path to a repository to read from. This is typically the directory that contains the logdata and tracedata directories.

*targetPath*

Specify the path at which to create a new repository. The *targetPath* must be specified.

**Note:** Either *serverName* or *repositoryPath* must be specified, as well as the *targetPath*.

Filter options:

All filters are optional. When multiple filters are used, they are logically ANDed together.

- `--minDate=value`  
Filter based on minimum record creation date. Value must be specified as either a date (for example `--minDate="2/20/13"`) or a date and time (for example `--minDate="2/20/13 16:52:32:808 EST"`).
- `--maxDate=value`  
Filter based on maximum record creation date. Value must be specified as either a date (for example `--maxDate="2/20/13"`) or a date and time (for example `--maxDate="2/20/13 16:52:32:808 EST"`).
- `--minLevel=value`  
Filter based on minimum level. Value must be one of the following: FINEST | FINER | FINE | DETAIL | CONFIG | INFO | AUDIT | WARNING | SEVERE | FATAL.
- `--maxLevel=value`  
Filter based on maximum level. Value must be one of the following: FINEST | FINER | FINE | DETAIL | CONFIG | INFO | AUDIT | WARNING | SEVERE | FATAL.
- `--includeLogger=value[,value]*`  
Include records with specified logger name. Value may include \* or ? as a wildcard.
- `--excludeLogger=value[,value]*`  
Exclude records with specified logger name. Value may include \* or ? as a wildcard.
- `--includeMessage=value`  
Filter based on message name. Value may include \* or ? as a wildcard.
- `--includeThread=value`  
Include records with specified thread id. Values must be in hexadecimal (for example, `--includeThread=2a`).
- `--includeExtension=name=value[,name=value]*`

Include records with specified extension name and value. Value may include \* or ? as a wildcard. To include a comma in the value, you must use "\",

- `--includeInstance=value`

Include records from the specified server instance. Value must either be "latest" or be a valid instance ID. Run this command using the listInstances action to see a list of valid instance IDs.

## listInstances

List the IDs of server instances in the repository. A server instance is the collection of all log/trace records written from the time a server is started until it is stopped. Server instance IDs can be used with the `--includeInstance` option of the binaryLog view action.

The command syntax is as follows:

```
binaryLog listInstances {serverName | repositoryPath}
```

*serverName*

Specify the name of a Liberty server with a repository to read from.

*repositoryPath*

Specify the path to a repository to read from. This is typically the directory that contains the logdata and tracedata directories.

**Note:** If *serverName* or *repositoryPath* are not specified on the command line, the task is performed against the default server instance, `defaultServer`, if it exists.

Be aware of binaryLog filtering optimizations. The binaryLog tool is able to filter log and trace data most efficiently when used with the following filter options:

- `--minDate`
- `--maxDate`
- `--includeThread`
- `--minLevel`
- `--maxLevel`

## Example usage

See the following examples of binaryLog commands.

- Display all events in the `defaultServer` repository between July 19th, 2013 and August 2nd, 2013.  

```
binaryLog view --minDate=07/19/13 --maxDate=08/02/13
```
- Display new events from server `myServer`, whose specified level is `WARNING` or higher, using the advanced format as the server writes them to the log repository.  

```
binaryLog view myServer --monitor --minLevel=WARNING --format=advanced
```
- Write log messages from a repository at `/apps/server1/logs`; include only those that were written to the error stream of a specific repository.  

```
binaryLog view /apps/server1/logs --includeLogger=SystemErr
```
- View events from the `defaultServer` repository that occurred before September 14th, 2012 4:28 PM eastern daylight time.  

```
binaryLog view --maxDate="09/14/12 16:28:00:000 EDT"
```
- Write events from the `defaultServer` repository that contain a 'thread' extension with value 'Default Executor-thread-4'  

```
binaryLog view --includeExtension=thread="Default Executor-thread-4" --format=advanced
```
- View the list of server instances in the `defaultServer` repository:  

```
binaryLog listInstances
```

Using `D:\wlp\usr\servers\defaultServer\logs` as repository directory.

Instance ID	Start Date
1358809441761	1/21/13 18:04:01:761 EST
1358864476191	1/22/13 9:21:16:191 EST

1358869523192	1/22/13 10:45:23:192 EST
1358871281166	1/22/13 11:14:41:166 EST
1358879829000	1/22/13 13:37:09:000 EST
1358892222067	1/22/13 17:03:42:067 EST

- View events from the defaultServer using one of the instance IDs from the previous example:

```
binaryLog view --includeInstance=1358871281166
```

- Copy events from the defaultServer, whose specified level is WARNING or higher, from the latest server instance to a new repository at d:\toSupport directory.

```
binaryLog copy defaultServer d:\toSupport --minLevel=warning --includeInstance=latest
```

## Configuring binary logging in Liberty

8.5.5.0

Use this information as a guide for configuring binary logging in your Liberty.

### About this task

Binary logging provides faster log and trace handling capabilities and more flexible ways to use log and trace content than the default Liberty log and trace framework.

A server configuration consists of a bootstrap.properties file, a server.xml file, and any (optional) files that are included with those files. The bootstrap.properties file specifies properties that need to be available before the main configuration is processed, and are kept to a minimum. The server.xml file is the primary configuration file for the server.

The server.xml file and its associated files use a simple xml format that is suitable for most text editors.

**Distributed operating systems** A richer editing experience is provided by the eclipse server adapter for Liberty (WAS4D+ adapter), which uses a generated schema to provide drop-down lists of available choices, auto-completion, and other editing tools. For a description of the eclipse server adapter for Liberty, see “Editing the Liberty configuration by using developer tools” on page 1556.

The bootstrap.properties file specifies whether the server uses binary logging as the log and trace framework, or the default log and trace framework. A server restart is required to switch between binary logging and the default log and trace framework.

You can modify the configuration of binary logging through the server configuration or the bootstrap.properties file.

- Server configuration: To get logging from your own code, which is loaded after server configuration processing, use the server configuration to configure binary logging.
- bootstrap.properties file: You might need to set logging properties to take effect before the server configuration files are processed. For example, if you need to analyze problems that occur early in server start or configuration processing. In this case, you can configure binary logging in the bootstrap.properties file.

You can set Logging properties in either the bootstrap.properties or the server.xml file. Use attributes in the server.xml file, or use equivalent properties in the bootstrap.properties file. Any settings in the bootstrap.properties file are used from the time the server reads the bootstrap.properties file until the time the server.xml file is processed. If the logging properties in the bootstrap.properties file are not replaced or reset in the server.xml file, the property values in the bootstrap.properties file continue to be used.

When binary logging is enabled, the **maxFileSize**, **maxFiles**, **messageFileName**, **traceFileName**, and **traceFormat** logging element attributes are ignored (since binary logging runs without trace.log and

messages.log files). The **traceSpecification**, **consoleLogLevel**, and **logDirectory** attributes continue to be used to set the trace specification, the level for the console log, and the placement of the log and trace files.

If you set logging or binary logging attributes in the server.xml file, you can avoid changes in configuration between startup time and runtime by setting the corresponding properties in the bootstrap.properties file to the same value. If no logging or binary logging properties are set in the bootstrap.properties file, the server uses the default logging settings.

## Procedure

- Enable binary logging for the server by updating the bootstrap.properties file. In the bootstrap.properties file, add the following text on a line by itself:  
websphere.log.provider=binaryLogging-1.0
- Use the following parameters to configure binary logging. All subelements that are listed are subelements of the logging element in the server.xml file. The following table lists the attributes that are configurable in the server.xml file and the equivalent properties that can be set in the bootstrap.properties file:

*Table 187. Binary logging attributes that are configurable in server.xml and the equivalent properties that can be set in bootstrap.properties*

Logging subelement	Attribute	Equivalent bootstrap.properties property
binaryLog	purgeMaxSize	com.ibm.hpel.log.purgeMaxSize
	purgeMinTime	com.ibm.hpel.log.purgeMinTime
	fileSwitchTime	com.ibm.hpel.log.fileSwitchTime
	bufferingEnabled	com.ibm.hpel.log.bufferingEnabled
	outOfSpaceAction	com.ibm.hpel.log.outOfSpaceAction
binaryTrace	purgeMaxSize	com.ibm.hpel.trace.purgeMaxSize
	purgeMinTime	com.ibm.hpel.trace.purgeMinTime
	fileSwitchTime	com.ibm.hpel.trace.fileSwitchTime
	bufferingEnabled	com.ibm.hpel.trace.bufferingEnabled
	outOfSpaceAction	com.ibm.hpel.trace.outOfSpaceAction

The following example shows a bootstrap.properties file that is configured to enable binary logging:  
websphere.log.provider=binaryLogging-1.0

The following example shows a server.xml file with the binary logging subelements. The log content is set to expire after 96 hours and the trace content is set to retain a maximum of 1024MB:

```
<server description="new server">
  <logging>
    <binaryLog purgeMinTime="96"/>
    <binaryTrace purgeMaxSize="1024"/>
  </logging>
</server>
```

For the full logging configuration reference, see the logging, binaryLog, and binaryTrace elements in the .

## Results

After you restart the server, binary logging is enabled and configured.

---

## Liberty:Runtime environment known issues and restrictions

There are some known issues and restrictions that apply when working with the Liberty runtime environment.

### Distributed operating systems

See also “Liberty: Developer Tools known issues and restrictions” on page 2342.

## Minimum supported Java levels

Liberty is supported with any compliant Java SE 6, Java SE 7, or Java SE 8 runtime environment (JRE) or Java SDK, subject to the minimum supported levels shown for the following specific implementations.

### Java SE 6 runtime environment

For the Java SDK from IBM, the minimum supported level is 6.0 (J9 2.6) SR 1. For the JDK from Oracle, the minimum supported level is Java 6 update 26.

### Java SE 7 runtime environment

For the Java SDK from IBM, the minimum supported level is IBM Runtime Environment, Java Technology Edition 7.0.4.1. For the JDK from Oracle on Windows and Linux, the minimum supported level is Java SDK/JRE/JDK 7.0.17. For the JDK from Oracle on Mac OS X, the minimum supported level is Java SDK/JRE/JDK 7.0 Update 15.

### 8.5.5.5 Java SE 8 runtime environment

For the Java SDK from IBM, the minimum supported level is IBM SDK, Java Technology Edition, Version 8. For the JDK from Oracle, the minimum supported level is Java 8 update 25.

### Distributed operating systems

On distributed platforms, 32-bit or 64-bit Java is supported. **z/OS** On the z/OS platform, only 64-bit Java is supported.

### Distributed operating systems

For Windows and Linux systems, you can use either the JDK from Oracle or the JDK from IBM. If you are developing applications on Windows or Linux, and you plan to deploy those applications to a server running on WebSphere Application Server classic, you should use the JDK from IBM. For HP systems and Mac OS, use the JDK from Oracle. **z/OS** For z/OS systems, use the JDK from IBM.

**Note:** **IBM i** To obtain the minimum supported Java level for IBM iSeries, install IBM J2SE 6.0 32-bit JVM (5761-JV1 option 11 **8.5.5.2** or 5770-JV1 option 11) or IBM SE 6.0 64 bit (5761-JV1 option 12 **8.5.5.2** or 5770-JV1 option 12), and also install Java PTF group SF99572 level 8 (or later) for IBM i 7.1.

## The installation directory name and path cannot include non-ASCII characters

Recent JVMs do not fully support use of non-ASCII characters with the **-jar** and **-javaagent** commands. You should use only ASCII characters in your installation directory names and paths.

## Changing the JDBC data source at run time might result in JPA failures

If the database dictionary type is not specified through properties, it is detected and calculated by OpenJPA when the first entity manager is created and the database connection is made. This database dictionary type is used for all entity managers that are subsequently created. If the JDBC data source is changed while an application is running, the entity manager factory does not detect this change and continues to use the old dictionary for operations against the new data source. This can result in failures if the database is changed to a different vendor.

When you change a database to a different vendor, restart the application.

## Modifying the dataSource, jdbcDriver, connectionManager, and JDBC vendor properties at run time might result in JPA failures

If you update the configuration of dataSource, jdbcDriver, connectionManager or any of the JDBC vendor properties lists (for example, properties.db2.jcc or properties.oracle) while the server is running, you might see J2CA8040E failures. These failures state that multiple dataSource elements cannot be associated with a single connectionManager. These failures are generated even if your configuration associates only one connectionManager with the dataSource element.

When you make updates to the configuration of any of these JDBC resources, restart the server.

## An application that relies on a result being returned by getRealPath must be deployed as an expanded application, not as a WAR file

The Java EE specification states that the getRealPath() method returns a null value if the content is being made available from a web archive (WAR) file. When you deploy a WAR file to Liberty, Liberty does not automatically extract the archive file into a directory structure. Therefore the application might fail to start. If your application relies on a result being returned by getRealPath(), you must deploy the application as an expanded web application, not as a WAR file. For example, you can manually extract the WAR file and copy the expanded application to the dropins directory.

## WebSphere Application Server traditional scripts do not work with Liberty

You cannot use any of the scripts under the bin directory of the WebSphere Application Server traditional to administer Liberty.

## Fileset restrictions

The following restriction applies to Filesets:

- Filesets do not recursively explore subdirectories of the base directory. For example, the following instructions are not supported:

```
<fileset id="testFileset" dir="\temp" includes="**\a.jar"/>
<fileset id="testFileset" dir="\temp" includes="a\a.jar"/>
<fileset id="testFileset" dir="\temp" includes="*\a.jar"/>
<fileset id="testFileset" dir="\temp" includes="a\b\a.jar"/>
```

## Overriding classes from the Java SDK

Some Java EE 6 technologies supported by Liberty require newer versions of APIs that are provided by Java SE 6. JAX-WS, JAXB and the javax.annotation.Resource annotation are all examples where a Java 6 SDK contains older classes than those required by Java EE 6. When compiling your application code against these APIs using Java SDK version 6, you need to use classes that are provided by Liberty rather than the Java SDK. You must take one of the following actions:

- If you are using javac to build from the command line, compile your code by using the javac -endorseddirs option and the JAR files in the \${wlp.install.dir}/dev/specs directory.
- If you are using Apache Ant to build, compile your code by using the <compilerarg> child element of the javac task and the JAR files in the \${wlp.install.dir}/dev/specs directory. In the build script, specify the -endorseddirs option and the \${wlp.install.dir}/dev/specs directory as separate <compilerarg> elements. For example:

```
<javac srcdir="src" destdir="classes"/>
  <compilerarg value="-endorseddirs"/>
  <compilerarg value="${wlp.install.dir}/dev/specs"/>
</javac>
```

- If you are using Apache Maven to build, compile your code by using the `endorseddirs` element of the Maven compiler plug-in and the JAR files in the `${wlp.install.dir}/dev/specs` directory. For example:

```
<plugin>
  <groupId>org.apache.maven.plugins</groupId>
  <artifactId>maven-compiler-plugin</artifactId>
  <configuration>
    <source>1.6</source>
    <target>1.6</target>
    <compilerArguments>
      <endorseddirs>${wlp.install.dir}/dev/specs</endorseddirs>
    </compilerArguments>
  </configuration>
</plugin>
```

Windows

## When you unpublish a shared library, it cannot be deleted until the server is stopped

When you unpublish a shared library from a server, the library JAR file is not immediately released from the server. Therefore the operating system does not know that the file is no longer in use, and does not let you delete the file. When you next stop the server, the library JAR file is released and you can delete the file.

z/OS

## Version 1.11 or later is required for Liberty on z/OS

To use the native z/OS capabilities of Liberty, you must use z/OS Version 1.11 or later.

z/OS

## z/OS APAR OA37620 is required to enable server tracing for a specific trace group

If you want to trace individual trace groups, apply z/OS APAR OA37620. When enabling tracing for Liberty on the z/OS platform, use the package/class syntax (that is, `com.ibm.ws.*=all`) unless directed otherwise by IBM support.

## java:global lookups restrictions

Resources defined in applications with `java:global` lookups can only be used to access names declared by applications deployed in the current server.

## appSecurity-2.0 feature restrictions

8.5.5.0

For the `appSecurity-2.0` feature, the following restrictions apply:

- For EJB applications, the **run-as-mode** of `SYSTEM_IDENTITY` is not supported in the extension settings of the `ibm-ejb-jar-ext.xml` file.
- The `getCallerIdentity` API is not supported for Singleton session beans.
- Role names can be referenced by the `HttpServletRequest.isUserInRole` and `EJBContext.isCallerInRole` APIs or by elements in the deployment descriptor without first declaring the role names using the `@DeclareRoles` annotation or the `<security-role/>` element in the deployment descriptor. However, roles must be declared before being used in WebSphere Application Server traditional.

## Applications not starting in an embedded Liberty server

Ensure that the Java process that starts the embedded Liberty server was started with the `-javaagent` JVM argument that pointed to the `libertyInstallDir/bin/tools/ws-javaagent.jar`. If the `-javaagent` JVM argument is not used the server runtime starts, but applications fail to start with no obvious exceptions.

8.5.5.6

## WebSphere MQ resource adapter and generic JCA support related restrictions

The WebSphere® MQ resource adapter can be used within the WebSphere Application Server Liberty by using either the `wmqJmsClient-1.1` or `wmqJmsClient-2.0` feature or by using generic JCA support.

You can use the WebSphere MQ resource adapter version 7.5 with Liberty version 8.5.5 and later. If you want to use WebSphere MQ resource adapter version 8.0, which is based on JMS 2.0 resource adapter, you must ensure that you are using the latest Liberty version that is compatible with the JMS 2.0 resource adapter.

### Notes:

- With Liberty version 8.5.5.2, the `wmqJmsClient-1.1` feature must be used with a IBM MQ resource adapter version 7.5.0.5 or later.
- With Liberty version 8.5.5.6, the `wmqJmsClient-2.0` feature must be used with a IBM MQ resource adapter version 8.0.0.3 or later

To know more about the version compatibility information between WebSphere MQ resource adapter and Liberty, see the Reference to obtain the WebSphere MQ resource adapter.

If you are using generic JCA support, the following restrictions apply:

- To run the IBM® WebSphere MQ resource adapter on z/OS, you must use the `wmqJmsClient-1.1` or `wmqJmsClient-2.0` feature.
- Tracing and logging are not integrated within the Liberty trace system using generic JCA. Trace is written to a separate file, and it must be enabled by setting the system properties. The procedure to enable tracing is the same as configuring the WebSphere MQ classes for JMS trace facility for a Java Standard Environment. See Java Standard Environment Trace stanza.
- The IBM MQ classes for Java are not supported in Liberty. They must not be used with either the IBM MQ Liberty messaging feature or with the generic JCA support. For more information, see Using WebSphere MQ Java Interfaces in J2EE/JEE Environments.

## Versioning is not possible for applications in the “dropins” directory

For applications in the “dropins” directory, the file name and file extension are used by the application monitor to determine the type of application, and to generate the application id and application name. It is therefore not possible to specify the version number for the application by using the file name or file extension. In a production environment, you are not recommended to use the “dropins” directory.

## Shared session applications must store session objects in shared libraries

When you are using the `shared-session-context` application extension, or `<shared-session-context value="true"/>` in `ibm-application-ext.xml`, all objects that are stored in the session must be available in the shared libraries that are associated with the application so that the session can be invalidated.

## Configuring session persistence

There is only one `server.xml` file for each server, not a `server.xml` file for each EAR or WAR file. You set session persistence in a database by adding:

```
<httpSessionDatabase id="SessionDB" dataSourceRef="SessionDS" ... />
```

In Liberty, this setting for the database applies to all EAR and WAR files. It is not possible to set up some databases with session persistence and others without.

## Ported locally transacted JMS sessions do not work in Liberty

In WebSphere Application Server traditional, you can develop applications to take advantage of locally transacted JMS sessions. When you port these applications to Liberty, these applications behave differently or do not work at all.

Even though WebSphere Application Server traditional allows locally transacted JMS sessions, porting a WebSphere Application Server traditional locally transacted JMS session to Liberty is not allowed.

## Admin Center feature restrictions

For the adminCenter-1.0 feature, the following restriction applies:

- **8.5.5.2** Using an IBM Java virtual machine (JVM) available with a WebSphere Application Server traditional product, such as Network Deployment, can cause WebSphere Liberty Administrative Center ("Admin Center") to not display in a browser. By default, the IBM JVM available with the WebSphere Application Server traditional product points to security classes that are available only with the WebSphere Application Server traditional product, and not to security classes needed by Admin Center, which requires Secure Sockets Layer (SSL). Use a JVM that supports Liberty products and SSL.
  - **8.5.5.4** You can get a JVM that supports Liberty products and SSL from Installation Manager offerings or developerWorks:
    - Using Installation Manager, select the Liberty product first and then select WebSphere SDK for Liberty. Use Installation Manager to install the Liberty product and software development kit (SDK). The WebSphere SDK for Liberty includes the needed support for Liberty products and SSL and offers a Java client, JConsole.
    - Go to <http://www.ibm.com/developerworks/java/jdk/index.html> on the developerWorks website and download an IBM Java development kit (JDK) for your operating system. The developerWorks website does not have a JVM for all operating systems. For example, you have to get the JDK from Eclipse for Windows operating systems.
- **8.5.5.4** From the Admin Center Deploy tool, you cannot use the **Use the connection method and credentials configured for each target host** option of **Remote Management Credentials** to deploy Liberty 8.5.5.3 or earlier server package to a registered host. The server package must support Liberty 8.5.5.4 or later.
- **8.5.5.5** The CPU Usage chart of the Admin Center Monitor view shows either **0%** or **null%** CPU usage for JVMs that do not supply process CPU statistics. For information about the chart, see "Monitoring metrics in Admin Center" on page 1754.

## Bean validation feature restrictions

For the beanvalidation-1.0 feature, the following restriction applies:

- There is no support for bean validation inside OSGi applications.

**8.5.5.6** For the beanValidation-1.1 feature, the following restrictions apply:

- There is no support for bean validation inside OSGi applications.
- Applications that provide a custom ConstraintValidatorFactory implementation in a validation.xml file with the beanValidation-1.0 feature do not compile against the Bean Validation 1.1 API.
- If a validation.xml file is not located in the module it is associated with, then there can be only one validation.xml file and the com.ibm.ws.beanvalidation.allowMultipleConfigsPerApp property must be set to false in either of the following files:

```
| - jvm.options
|   -Dcom.ibm.ws.beanvalidation.allowMultipleConfigsPerApp=false
| - bootstrap.properties
|   com.ibm.ws.beanvalidation.allowMultipleConfigsPerApp=false
```

## Dynamic cache feature restrictions

### 8.5.5.0

The following dynamic cache features are not available or have limited availability:

- Cache replication is not supported.
- Only high performance disk caching mode is supported with random and size based eviction techniques.
- There is no support for Web Services client and server side caching as well as portlet cache in the `cachespec.xml` file.
- There is no support for servlet caching of `SingleThreadModel` servlets.
- Defining cache configuration by using properties files is not supported for JAR files that contain only Enterprise JavaBeans (EJBs).
- Limiting a heap cache size works only for 32-bit Java virtual machines (JVM).

## ejbLite-3.1 feature restrictions

### 8.5.5.0

For the `ejbLite-3.1` feature, the following restrictions apply:

- EJB modules prior to version 3.0 are not supported. This restriction also means that bindings and extensions using the `.xmi` file format rather than the `.xml` file format are not supported.
- Session beans are not bound to the `ejblocal` namespace, which means JNDI lookups and `ejb-ref` binding names must use `java:global`, `java:app`, or `java:module` names. The `simple-binding-name` and `interface-binding-name` elements are ignored in `ibm-ejb-jar-bnd.xml` files.
- The stateful bean passivation directory is not configurable. Files are passivated to the server work area.

### 8.5.5.6

## j2eeManagement-1.1 feature restrictions

For the `j2eeManagement-1.1` feature, the following restriction applies:

- The Management EJB `getListenerRegistry()` method is not supported. You cannot register an event notification listener in a Management EJB component.

### 8.5.5.0

## jaxb-2.2 feature restriction

For the `jaxb-2.2` feature, the following restrictions apply:

- If your application requires JAXB API classes and has already been started, and the `jaxb-2.2` server feature is to be enabled, you must restart the server with the `--clean` option so that your application can call the JAXB 2.2 API and implementation classes that are provided by the `jaxb-2.2` feature. Otherwise, your application might still bind to the JAXB API and implementation classes that are provided in the Java SDK.
- If the `jaxb-2.2` server feature is enabled, and you want to use your own JAXB API and implementation classes in your application, you must place your own JAXB API and implementation JAR files into the `/WEB-INF/lib` directory of your application, and configure the class loader of your application to use *parentLast* delegation behavior. Other wise, the JAXB API and implementation classes that are provided by the `jaxb-2.2` feature always take effect. For more information of configuring class loader behavior for you applications on Liberty, see “Overriding a provided API with an alternative version” on page 1600.

## 8.5.5.0

### jaxws-2.2 feature restrictions

For the jaxws-2.2 feature, the following restrictions apply:

- If your application provides its own copy of CXF JAR files as the application libraries, for example, in the WEB-INF/lib directory of a web application, you cannot enable the jaxws-2.2 feature in the server.xml file.
- Because the jaxws-2.2 feature depends on the jaxb-2.2 feature, the jaxb-2.2 feature restrictions also apply to the jaxws-2.2 feature.
- If your application requires JAX-WS API classes and has already been started, and the jaxws-2.2 server feature is to be enabled, you must restart the server with the --clean option so that your application can call the JAX-WS 2.2 API and implementation classes that are provided by the jaxws-2.2 feature. Otherwise, your application might still bind to the JAX-WS API and implementation classes that are provided in the Java SDK
- The web services binding file for Liberty is the ibm-ws-bnd.xml file. The following web services binding files for WebSphere Application Server traditional are not supported:
  - ibm-webservices-ext.xml
  - ibm-webservices-bnd.xml
  - ibm-webservicesclient-ext.xml
  - ibm-webservicesclient-bnd.xml
  - ws-security.xml
- The Apache Axis2 configurations or classes are not supported.
- The web service providers that implement javax.xml.ws.Provider<OMElement> or javax.xml.ws.Provider<String> interface are not supported.
- The **content-id** attribute of MIME attachments must be enclosed with angle brackets for Liberty. For example, <testID>.
- The **-inlineSchemas** option is not supported by the **wsgen** tool that is provided by Liberty.
- Enable MTOM if you want to transfer big binary data using JAX-WS web services to avoid the Out of Memory (OOM) error.
- For web service applications, if the service client and service provider are not in the same application and the WSDL file in the service provider application is changed, you need to restart the web service client application manually to avoid the WSDL definition cache issue.

## 8.5.5.6

### jpa-2.1 feature restrictions

For the jpa-2.1 feature, JPA entity exchange over CORBA/RMI-IIOP requires that both participants in the communication must enable identical JPA feature levels.

### jsp-2.2 feature restrictions

For the jsp-2.2 feature, the following restriction applies:

- There is no support for the useInMemory configuration option to only store the translated JSP file in memory.

## 8.5.5.9

### logstashCollector-1.0 feature restrictions

The following limitations apply to the logstashCollector-1.0 feature:

- Data Loss – Some events that are generated in Liberty might not be forwarded to Logstash as expected. Data loss might occur under the following scenarios:

1. Starting the Liberty server before the Logstash server is started. It is recommended that you start the Logstash server before starting the Liberty server.
  2. Heavy load conditions. Events might be dropped in cases where events are created in Liberty faster than they can be processed by Liberty's event pipeline, Logstash, and any other downstream consumers. Liberty uses buffers to avoid data loss when event creation is briefly faster than event consumption.
- The `logstashCollector-1.0` feature is tested and is compatible with Logstash V2.x.

#### 8.5.5.0

### **monitor-1.0 feature restriction**

For the `monitor-1.0` feature, the following restriction applies:

- When the feature is removed from the `server.xml` file, you must restart the server to make the JAX-WS applications work.

#### 8.5.5.6

### **requestTiming-1.0 feature restrictions**

For the `requestTiming-1.0` feature, the following restriction applies:

- The `requestTiming-1.0` feature, when activated, has been shown to have an 4% impact on maximum possible application throughput when measured with the DayTrader application. While the impact on your application might be more or less than that, you should be aware that some performance degradation might be noticeable.

#### 8.5.5.6

### **restConnector-1.0 feature restriction**

For the `restConnector-1.0` feature, the following restriction applies:

- Users of the `restConnector-1.0` feature or any feature that includes `restConnector-1.0`, such as `collectiveMember-1.0` and `collectiveController-1.0`, who want to run applications containing a custom JAXRS 2.0 runtime must add the `jaxrs-2.0` feature to that server.

#### 8.5.5.8

### **scim-1.0 feature restrictions**

The following restrictions apply for the `scim-1.0` feature:

- The `members` attributes are not retrieved while searching for groups.
- The `groups` attributes of users are not retrieved while searching for users.
- The Canonical type of `direct/indirect` cannot be set for groups attribute of users.
- Only one `email` attribute of user of Canonical type, `work`, can be defined.
- Only one `ims` attribute of user of Canonical type, `work`, can be defined.
- Extended schema attributes of SCIM such as `entitlements`, `roles` and `x509Certificates` cannot be set or returned.
- The `userName` attribute cannot be used with some other attributes in a filter.
- For users in Basic and SAF registries, only `userName`, `displayName`, `id`, `schema`, `meta.location` and `groups` can be set. The `userName` and `displayName` will have the same value.
- List/query with Basic and SAF registries does not work the same as the `ldapRegistry` registry.
- Operators like `pr`, `gt`, `ge`, `lt`, `le`, `and`, `or`, and `()` will not work with Basic and SAF registries. Also, only one operator must be used in the filter for Basic and SAF registries.
- Basic and SAF are read only registries.
- While creating user, `groups` attribute cannot be set.

## wmqJmsClient-1.1 feature restrictions

8.5.5.0

For the wmqJmsClient-1.1 feature, the following restrictions apply:

8.5.5.0

- You must manually set the PATH variable in the Windows environment variables to point to the IBM MQ installation bin directory. You must set this path variable when the application uses the BINDING connection mode.
- The IBM MQ classes for Java (generally called the Base Java) are not included in the wmqJmsClient-1.1 feature. This is included in the Resource Adapter for other application servers but is not recommended for the Base Java APIs in the Java Enterprise Edition environments. For more information, see Using IBM MQ Java Interfaces in J2EE/JEE Environments.
- The BINDINGS\_THEN\_CLIENT transport type of IBM MQ resource adapter is not supported for the wmqJmsClient-1.1 feature.
- The Advanced Messaging Security (AMS) feature is not included for the wmqJmsClient-1.1 feature.

8.5.5.6

## wmqJmsClient-2.0 feature restrictions

For the wmqJmsClient-2.0 feature, the following restrictions apply:

- You must manually set the PATH variable in the Windows environment variables to point to the IBM MQ installation bin directory. You must set this path variable when the application uses the BINDING connection mode.
- The IBM MQ classes for Java (generally called the Base Java) are not included in the wmqJmsClient-2.0 feature. This is included in the Resource Adapter for other application servers but is not recommended for the Base Java APIs in the Java Enterprise Edition environments. For more information, see Using IBM MQ Java Interfaces in J2EE/JEE Environments.
- The BINDINGS\_THEN\_CLIENT transport type of IBM MQ resource adapter is not supported for the wmqJmsClient-2.0 feature.

## collectiveController-1.0 feature restriction

8.5.5.0

If you start a collective controller server and then change your IP configuration, the controller no longer functions correctly.

## concurrent-1.0 feature restrictions

8.5.5.4

For the concurrent-1.0 feature, the following restrictions apply:

For the thread context of type securityContext, any custom information in the subject that was not added by using a JAAS login module will not be propagated. For example, if the submitter's subject contains a custom Principal that was added by a TAI, the propagated subject will not contain this custom Principal.

8.5.5.6

## jacc-1.5 feature restrictions

For the jacc-1.5 feature, the following configurations are ignored:

- Authorization information (the users and groups attributes of the authorizations attribute) in an ibm-application-bnd.xml file or an ibm-application-bnd.xmi file of the application's ear file.
- Authorization information (the user, group and special-subject attributes of the security-role attribute in the application-bnd element) in the server.xml file.

---

## Liberty: Developer Tools known issues and restrictions

### Distributed operating systems

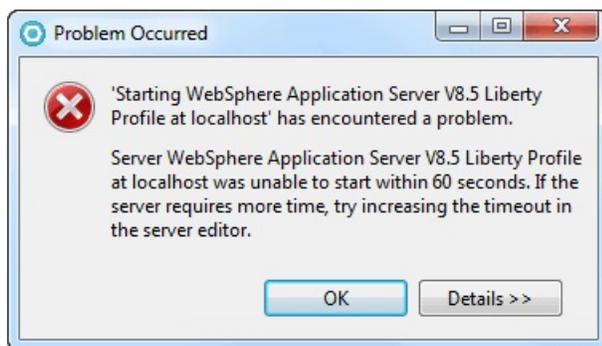
Several known issues and restrictions apply when you are working with WebSphere Application Server Developer Tools for Eclipse.

See also “Liberty:Runtime environment known issues and restrictions” on page 2333.

### 8.5.5.0

## Unable to interact with the Liberty server after you modify the console log level settings

There is a known limitation when the console log level is set to WARNING, ERROR, or OFF. The workbench has problems when it interacts with the Liberty server, such as cannot start, stop, or publish to the server. For example, the workbench is unable to start the Liberty server and the following timeout error message displays:



The console log level (`consoleLogLevel`) is an attribute of the logging configuration element in the server configuration (`server.xml`) file with the following range options: INFO, AUDIT, WARNING, ERROR, and OFF. AUDIT is the default value for the console log level settings. For more details, search for the `consoleLogLevel` attribute in the topic.

To work around this known limitation, specify INFO or use the default AUDIT setting for the console log level:

1. In the Servers view, expand your Liberty server.
2. Right-click the **Server Configuration[server.xml]** node and select **Open**.
3. In the Server Configuration editor and under the **Configuration Structure** section, expand **Server Configuration** node. The next step depends if the **Logging** element is available:
  - If the **Logging** element is available, select it and under the **Logging** section of the server configuration editor, use the drop-down menu for the **Console log level** field, and select either the AUDIT or INFO option. Type `Ctrl + s` to save your changes in the editor.
  - If the **Logging** element is not available, the workbench is already using the default AUDIT setting. As a result, you might be experiencing a different problem that is causing interaction failures between the workbench and the Liberty server.

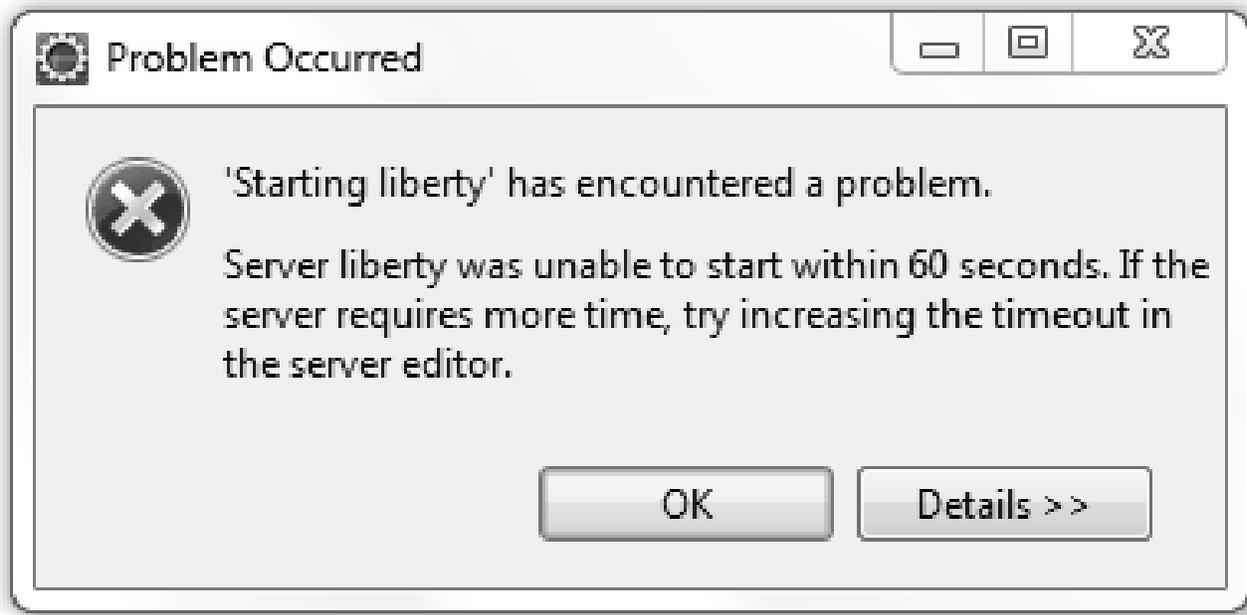
## Copying and pasting servers might cause the publishing state to become out of synchronization

Try to avoid copying and pasting servers because they point to the same configuration file. Copying and pasting servers might cause the publishing state to become out of synchronization. For example, when you remove an application from one server, the application still appears to be deployed to the other server even though it is not. Server state will not synchronize up again until the next publish operation.

8.5.5.4

### Unable to recognize the start of the server when the hideMessage attribute is used to suppress the messages

You can configure the <hideMessage> attribute in the Logging element of **Server Configuration** [server.xml] to suppress messages. If you configure to hide the server start message, for example <logging hideMessage="CWWKF0011I"/>, then the tool fails to recognize the state of the server when it is started. In such a situation, the state of the server in the **Server** view remains as *starting* until timeout and finally displays the following message:



8.5.5.4

### Remote servers cannot run projects that were created with a newer version of Java

If you compile a project with a higher version of Java than your remote server is running, you can receive the following error messages:

```
Error 404: javax.servlet.UnavailableException:  
SRVE0202E: Servlet [s1]: s1 was found, but is corrupted:  
SRVE0227E: Check that the class resides in the proper package directory.  
SRVE0228E: Check that the classname has been defined in the server using the proper case and fully qualified package.  
SRVE0229E: Check that the class was transferred to the filesystem using a binary transfer mode.  
SRVE0230E: Check that the class was compiled using the proper case (as defined in the class definition).  
SRVE0231E: Check that the class file was not renamed after it was compiled.
```

If you create a project in a package with a higher version of Java than your remote server is running, you can receive the following error messages:

```

Error 404: java.io.FileNotFoundException: SRVE0190E: File not found: /s2
Console output: [ERROR ] SRVE0266E: Error occurred while initializing servlets: java.lang.UnsupportedClassVersionError:
at java.lang.ClassLoader.defineClassImpl(Native Method)
at java.lang.ClassLoader.defineClass(ClassLoader.java:383)
at com.ibm.ws.classloading.internal.AppClassLoader.definePackageAndClass(AppClassLoader.java:318)
at [internal classes]

```

To avoid these errors, compile your project with the same version of Java that your remote server is running, or with an earlier version. You can also create your project in a package with the same version of Java that your remote server is running, or with an earlier one. To find the Java version of the remote server, check the `messages.log` file. For more information about viewing the `messages.log` file, see “Viewing trace and message log files by using developer tools” on page 2317.

8.5.5.10

## Some utilities are unavailable when you use a remote Liberty server or a Liberty server in a Docker container

WebSphere Developer Tools do not support some of the utilities when you use a remote Liberty server or Liberty server in a Docker container.

The tools do not support the following utilities when you use a remote Liberty server:

- **Generate Web Server Plug-in...**
- **Add Config Snippets...**

The tools do not support the following utilities when you use a Liberty server in a Docker container:

- **Generate Web Server Plug-in...**
- **Package Server...**
- **Create Collective...**
- **Add Config Snippets...**

---

## Liberty:Messages

When you use Liberty, you might encounter system messages. Each message has a unique message identifier, and includes an explanation of the problem, and details of any action that you can take to resolve the problem.

Liberty system messages are logged from various sources, including application server components and applications. For Liberty, the message identifier is 10 characters in length and has the following form:

CWXXX9999X

where:

**CWXXX**

Is a five-character alphabetic message prefix that identifies the Liberty component.

**9999** Is a four-character numeric identifier used to identify the specific message for that component.

**X** Is an optional alphabetic indicator that identifies the message type: I=Informational, W=Warning, E=Error.

*Table 188. Alphabetic message prefixes for Liberty messages*

Liberty message prefix	Range	Liberty component
CWIMK	0001-0500	LDAP registry federation (configuration messages)
CWIML	0001-5000	LDAP registry federation (runtime messages)

Table 188. Alphabetic message prefixes for Liberty messages (continued)

Liberty message prefix	Range	Liberty component
CWLIB	0001-0100	Transactions
	0101-0200	z/OS Transaction Extensions
CWWKB		<i>z/OS Native integration</i>
	0001-0050	z/OS Command Processing
	0051-0100	z/OS Native code only
	0101-0150	z/OS Core
	0151-0200	z/OS WLM services
	0201-0250	z/OS Native code non-console
CWWKC	0000-0250	Annotation scanning
CWWKE		<i>Core kernel and kernel services</i>
	0001-0099	Boot/Launcher
	0100-0199	Service utilities
	0200-0299	Location service
	0300-0399	File installation service
	0400-0499	FileMonitor service
	0500-0599	Extensible Class Scanner
CWWKF		Feature manager
CWWKG		Configuration manager
CWWKJ		Light touch administration
CWWKL	0001-0100	Class loading service
CWWKM	0001-0050	Artifact API messages (container factory)
	0051-0100	Overlay Messages (all implementations)
	0101-0150	Artifact API Zip implementation
	0151-0200	Artifact API File implementation
	0401-0450	Adaptable API Implementation messages (adaptable module factory / adapter service)
	1001-1100	Loose archive API (used by the Eclipse-based tools option that runs an application directly from the Eclipse workspace(The Eclipse platform supports a "virtual" application archive, where a set of files that appear to be in the same archive file are actually spread out across the Eclipse workspace. Liberty calls this a "loose archive", and the tools option that uses the loose archive API is called <b>Run this application directly from the workspace</b> )).
	2000-2999	Ant and Maven plug-in
CWWKN	0001-0100	JNDI default namespace

Table 188. Alphabetic message prefixes for Liberty messages (continued)

Liberty message prefix	Range	Liberty component	
CWWKO		CFW components	
	0000-0199	CFW	
	0200-0399	TCP	
	0400-0599	UDP	
	0600-0799	bytebuffer	
	0800-0899	SSL channel	
	0900-0999	SSL	
CWWKS		Security	
	0000 series		Security: General messages
		0000-0099	Security
		0900-0999	Security quickStart
	1000 series		Security: Authentication services
		1000-1099	Authentication
		1100-1199	JAAS authentication
		1200-1299	TAI authentication
	2000 series		Security: Authorization services
		2000-2099	Authorization
		2100-2199	Built-in authorization
		2900-2999	SAF authorization
	3000 series		Security: Registry services
		3000-3099	Registry
		3100-3199	Basic registry
		3200-3299	LDAP registry
		3300-3399	FileBased (VMM) registry
		3800-3899	Custom registry
		3900-3999	SAF registry
	4000 series		Security: Token services
		4000-4099	Token services
		4100-4199	LTPA
		4200-4299	Kerberos
		4300-4399	SPNEGO
	9000 series		Security: Collaborators
		9100-9199	Web Collaborator (common code)
		9200-9299	Web Application Collaborator
9300-9399		Web Administration Collaborator	
CWWKT		HTTP transport/dispatcher	

Table 188. Alphabetic message prefixes for Liberty messages (continued)

Liberty message prefix	Range	Liberty component
CWWKW	0000-0099	JAX-WS common
	0100-0199	JAX-WS for webContainer
	0200-0299	JAX-WS security
	0300-0399	JAX-WS for Java EE common
CWWKX	0000 series	JMX
	0001-0100	JMX Security
	0101-0200	JMX REST Connector
	0201-0300	JMX REST Client
	8.5.5.3 1000 series	Administrative Center
	8.5.5.3 1000-1899	Admin Center
CWWKZ		Applications
	0001-0100	Application manager
	0101-0200	WARs
	0201-0300	WABs
	0301-0400	EBAs

## Liberty: Abend reason codes

z/OS

When you use Liberty, you might encounter abend reason codes. Each message has a unique message identifier, and includes an explanation, and details of any action that you can take.

**Note:** Abend reason codes that are not listed in this chapter must be reported to the IBM Support Center.

Table 189. Liberty for z/OS abend codes

Abend code	Abend reason	Explanation	Suggested action
EC3 hex	20000005	The BBGZSAFM module cannot be loaded from the file system.	Make sure that Liberty is installed without errors, and that the user ID running Liberty server has permission to read the files in Liberty installation. If the problem persists, contact your next level of support.
EC3 hex	20000006	The BBGZSAFM module is not APF-authorized.	Make sure that Liberty is installed without errors. The BBGZSAFM module must have been installed with the APF authorization bit set. If the problem persists, contact your next level of support.

Table 189. Liberty for z/OS abend codes (continued)

Abend code	Abend reason	Explanation	Suggested action
EC3 hex	20000007	A call to UNIX System Services stat function to the BBGZSAFM load module failed.	Make sure that Liberty is installed without errors, and that the user ID running Liberty server has permission to read the files in Liberty installation. If the problem persists, contact your next level of support.
EC3 hex	20000008	The path name to the BBGZSAFM module in the file system is too long. The path cannot be more than 4096 characters.	Install Liberty to the file system that can be accessed with a shorter PATH.
EC3 hex	20000009	The size of the BBGZSAFM module is smaller than the minimum size for this load module.	Make sure that Liberty is installed without errors. If the problem persists, contact your next level of support.
EC3 hex	2000000A	The size of the BBGZSAFM module is smaller than the minimum size for this load module based on the number of functions it contains.	Make sure that Liberty is installed without errors. If the problem persists, contact your next level of support.

## Troubleshooting OSGi applications by using developer tools

### 8.5.5.9

You can configure the `osgiAppConsole-1.0` feature with WebSphere Developer Tools and then use it to determine and analyze the OSGi applications-related issues.

### Before you begin

- Install WebSphere Developer Tools for Eclipse and WebSphere Application Server Liberty. You can install the tools by using downloaded installation files. For more information about installing WebSphere Developer Tools and Liberty, see “Installing Liberty developer tools and (optionally) Liberty” on page 1374.
- Deploy an OSGi application to a running Liberty server.
- The `osgiAppConsole-1.0` feature is available as part of the downloaded compressed files. If the feature is not already installed, then install the feature from the Liberty Repository by using the following command:

```
bin\installUtility install osgiAppConsole-1.0
```

### Procedure

1. Configure the `osgiAppConsole-1.0` feature in the `server.xml` file.

```
<featureManager>
  <feature>osgiAppConsole-1.0</feature>
</featureManager>
```

2. Add the security configurations.

The following example shows a sample security configuration with an admin role that uses basic authorization and HTTPS security.

```
<httpEndpoint httpPort="9080" httpsPort="9443" id="defaultHttpEndpoint"/>
<keyStore id="defaultKeyStore" password="Liberty"/>
<quickStartSecurity userName="admin" userPassword="password"/>
```

3. Start the OSGi Application Console or the OSGi Shared Bundle Console by completing one of the following tasks.
  - Start the OSGi Application Console:
    - a. In the Servers view, right-click the OSGi module.
    - b. Select **Launch OSGi Application Console**.The tools open a browser that displays the OSGi Application Console page.
  - Start the OSGi Shared Bundle Console:
    - a. Right-click your server.
    - b. Select **Utilities > Launch OSGi Shared Bundle Console**.The tools open a browser that displays the OSGi Shared Bundle Console page.

---

## Troubleshooting Session Initiation Protocol (SIP) on Liberty

Troubleshoot SIP by using the available log and trace facilities. You can use the default log and trace facility, or you can enable binary logging for high-performance, extensible logging and tracing.

### Troubleshooting the SIP container session repository on Liberty

8.5.5.7

When you troubleshoot the SIP container session repository, you might need the SIP session details to dump to a specified trace file.

#### About this task

You can use the SIP session memory dump utility to help debug problems that are related to SIP container sessions. The SIP container provides the `SipContainerMBean` method to perform several serviceability type operations on the SIP container, including the initiation of a server quiesce through the command line. This task describes how you can use the `SipContainerMBean` method to dump SIP application session and SIP session information that is contained in the in-memory session repository for SIP containers. By configuring the `SIPContainerMBean` method to use various trace methods, you can specify the SIP session details to dump to the specified trace file.

When the session dump methods are started, the requested information about the sessions prints by default into the `console.log` file. You can also send the information to a predefined source specified on the `setDumpMethod` method.

You can run the dumping utility in two modes, *succinct* and *verbose*. When you use the succinct session dump methods, only the session IDs are printed for every dump method execution. If you want to use the verbose session dump methods, the following actions occur:

- Transaction user details, along with the SIP session details, if they exist, print for every dump method execution.
- The only attributes that dump to the trace file are those attributes that the JSR 289 specification permits for exposure.
- The verbose methods print the following information in the trace file: `appName`, `callID`, `dialog state`, `creation time`, `attribute names`.

The trace printouts occur per SIP application; therefore, the sorting of all the SIP session data structures occurs before printing. The `SIPContainerMBean` dump facility runs in a low-priority thread so that the tracing does not affect the call processing latency of the overall system for a production server.

The dump distinguishes between a transaction user that has a SIP session versus a transaction user that has no SipSession object. Also included in the dump, in a delineated fashion, are SIP sessions that no longer exist, that are no longer valid, or that exist at the time of the trace snapshot.

On Liberty, you can invoke the SipContainerMBean dumping methods in two ways:

- By running the **server dump** command
- By implementing a Java Management Extensions (JMX) client that establishes a connection to the JMX connector to invoke the methods

The following succinct SipContainerMBean methods are used to dump SIP session IDs.

*Table 190. Succinct SipContainerMBean methods used to dump SIP session information.*

Method	Description
dumpAllSASIDs()	Prints a number of all SIP application sessions and the SIP application session IDs.
dumpAllTUSipSessionIds()	Prints a number of transaction users and the SIP session IDs within the transaction user (TU), if one exists.

The following verbose SipContainerMBean methods are used to dump SIP session details.

*Table 191. Verbose SipContainerMBean methods used to dump SIP session information.*

Method	Description
dumpAllSASDetails()	Prints a number of all SIP application sessions and the SIP application session ID details.
dumpAllTUSipSessionDetails()	Prints a number of transaction users and details of the SIP session IDs within the transaction user (TU), if one exists.
dumpSASDetails(String sasId)	Prints the details of the SIP application session that is specified by the sasId parameter.
dumpSipSessionDetails(String sessionId)	Prints the details of the SIP session that is specified by the sessionId parameter.

**Note:** Use the following information to help parse print output:

- For all print output, the first line provides an application name and a number of records.
- The delimiter between the output is a TAB.
- The delimiter between session attributes is a ; (semi-colon).

## Procedure

- Invoke the SipContainerMBean methods with the **server dump** command. For more information about the **server dump** command, see “Generating a Liberty server dump from the command line” on page 1579.

1. In the server.xml file, specify the dumping utility mode on a sipIntrospect element.

- For succinct mode, specify the following code:

```
<sipContainer>
  <sipIntrospect method="SUCCINCT"/>
</sipContainer>
```

- For verbose mode, specify the following code:

```
<sipContainer>
  <sipIntrospect method="VERBOSE"/>
</sipContainer>
```

2. Open a command line and change to the wlp/bin directory.

- To generate the SIP sessions and SIP application sessions dump, run the following command, where *server\_name* is the Liberty server:

```
server dump server_name
```

If you do not specify a server name, defaultServer is used.

You can optionally specify the name of the server dump package file on the **archive** parameter:

```
server dump server_name --archive=package_file_name.dump.zip
```

After you run the command, the server dump package file is generated and contains the following files:

- SipContainerIntrospector.txt, which includes the requested level of trace information about the SIP application sessions and SIP sessions
- Other *artifact*Introspector.txt files, which provide the server status information

SipContainerIntrospector.txt includes the following information, where dump.ids.test.appl is the application name, 2 is the number of sessions, and the local.##### lines are the SAS\_ids:

The description of this introspector:  
SIP state details

Succinct dumping

```
dump.ids.test.appl 2
local.1347524282775_8
local.1347524282775_7
```

--- End of Dump ---

- Invoke a specific dumping utility method through JMX connectors. For more information, see “Connecting to Liberty by using JMX” on page 1641 and “Developing a JMX Java client for Liberty” on page 1645.

The following Java code example invokes the dumpAllSASIDs method:

```
System.setProperty("javax.net.ssl.trustStore", "..\\wlp\\usr\\servers\\SIPServer\\resources\\security\\key.jks");
System.setProperty("javax.net.ssl.trustStorePassword", "Liberty");
```

```
//If the type of the trustStore is not jks, which is default,
//set the type by using the following line.
System.setProperty("javax.net.ssl.trustStoreType", "jks");
```

```
try {
    HashMap<String, Object> environment = new HashMap<String, Object>();
    environment.put("jmx.remote.protocol.provider.pkgs", "com.ibm.ws.jmx.connector.client");
    environment.put("com.ibm.ws.jmx.connector.client.disableURLHostnameVerification", Boolean.TRUE);
    environment.put(JMXConnector.CREDENTIALS, new String[] { "theUser", "thePassword" });
    environment.put(ConnectorSettings.DISABLE_HOSTNAME_VERIFICATION, true);

    JMXServiceURL url = new JMXServiceURL("service:jmx:rest://localhost:9443/IBMJMXConnectorREST");
    JMXConnector connector = JMXConnectorFactory.newJMXConnector(url, environment);
    connector.connect();
    MBeanServerConnection connection = connector.getMBeanServerConnection();

    // test dumping utility
    connection.invoke(new ObjectName("WebSphere:name=com.ibm.ws.sip.container.SipContainerMBean"), "dumpAllSASIDs",
```

Succinct SipContainerMBean methods have the following print formats.

Table 192. Succinct SipContainerMBean method print formats.

Method	Print format
dumpAllSASIDs()	Each line represents a SIP application session ID, in the format [SAS_ID].  For example: local.1347524282775_8

Table 192. Succinct SipContainerMBean method print formats (continued).

Method	Print format
dumpAllTUSipSessionIds()	Each line represents the transaction ID, whether the transaction has a SIP session, and the session ID if it exists, in the format [TU_ID] [hasSIPSession] [SipSessionId]  For example: local.1349965420866_1_0 true local.1349965420866_1_0_1

Verbose SipContainerMBean methods have the following print formats.

Table 193. Verbose SipContainerMBean method print formats.

Method	Description
dumpAllSASDetails()	Each line represents the SIP application session ID, the creation time, and the SIP session attributes, in the format [SAS_ID] [CreationTime] [attributes]  For example: local.1348147884986_2 Sep 20,2012 16:31 DumpSasDetailsAttr;
dumpAllTUSipSessionDetails()	Each line represents the transaction ID, whether the transaction has a SIP session, and the session details if it exists, in the format [TU_ID] [hasSIPSession] [SipSessionId] [Call-Id] [DialogState] [hasOutgoingTransaction] [initialMethod] [SAS_ID] [CreationTime] [attributes]  For example: local.1349965420866_1_0 true local.1349965420866_1_0_1 8-8548@9.148.57.128 2 false INVITE local.1349965420866_1 Jan 24,2013 14:41 TestSSAttr1; TestSSAttr2;
dumpSASDetails(String sasId)	Only one line is printed, in the format [TU_ID] [hasSIPSession] [SipSessionId]  For example: local.1349965420866_1_0 true local.1349965420866_1_0_1  If the requested session does not exist, the following error message is printed: ERROR: Requested session <local.1349965420866_1_0_1> does not exist.
dumpSipSessionDetails(String sessionId)	Only one line is printed, in the format [SipSessionId] [Call-Id] [DialogState] [hasOutgoingTransaction] [initialMethod] [SAS_ID] [CreationTime] [attributes]  For example: local.1349965420866_1_0_1 8-8548@9.148.57.128 2 false INVITE local.1349965420866_1 Jan 24,2013 14:41 TestSSAttr1; TestSSAttr2;  If the requested session does not exist, the following error message is printed: ERROR: Requested session <local.1349965420866_1_0_1> does not exist.

## Tracing a Session Initiation Protocol (SIP) container on Liberty

8.5.5.7

You can trace a Session Initiation Protocol (SIP) container, starting either immediately or after the next server start. This tracing writes a record of SIP events to a log file.

## Procedure

In the `server.xml` file, add a logging element and specify tracing for the SIP container by setting `traceSpecification="*=info:com.ibm.ws.sip=all"`.

```
<logging logDirectory="${server.config.dir}/logs" traceFileName="trace.log" traceSpecification="*=info:com.ibm.ws.sip=all"/>
```

## Results

SIP-level tracing messages appear in `serverName/logs/trace.log`, where `serverName` is the name of the specific instance of the application server that is running the SIP container to be traced. These messages include application load events as well as SIP request and response parsing and SIP servlet invocation.

## Session Initiation Protocol (SIP) binary log and trace extensions on Liberty

8.5.5.7

Binary logging provides a way for developers to add extension fields to log and trace records, and a corresponding way for you to filter log and trace records by extension value.

Log and trace records contain fields for information such as the time the record was created and the content of the message that is logged. These fields are core fields that are present in every log and trace record. In contrast, extension fields are fields which application developers can add to log and trace records, which you can use as filter criteria when you search for specific log and trace content. These log and trace extensions are visible in the binary log when you configure the text output format to use the advanced format, or they are visible when you use the `binaryLog` command in the advanced format.

### Administrators

The application server automatically creates a number of extensions that you can use to filter log and trace records. You can also filter log and trace records by using any extensions that are added by your application developers. You can use the `binaryLog` command-line tool to filter records based on the content of log and trace record extensions. For more information, see “BinaryLog command options” on page 1027.

For example, to see all SIP application sessions that the SIP container processed, you can use the following `binaryLog` command:

```
binaryLog view binaryFile --includeExtension=SIPASId=* --format=advanced
```

### Developers

Developers can use binary logging to add custom extensions to log and trace records through the log record context API, `com.ibm.websphere.logging.hpel.LogRecordContext`. When binary logging stores log and trace records, it includes any extensions that are present in the log record context on the same thread. For example, you can write a servlet filter to add important HTTP request parameters to the log record context. While that servlet runs, the HPEL API adds those extensions to any log and trace records that are created on the same thread.

As with other log and trace record fields, developers can access the record extensions by using the HPEL API. This API is useful when you write tools to read from log and trace repositories. Developers can also use the log record context API to access extensions in custom log handlers, filters, and formatters at run time.

The following table describes the log and trace extensions, including the identifier that you can use to filter various aspects of the trace.

Table 194. Log and trace extensions.

Extension	Description
appName	Specifies the name of the Java Platform, Enterprise Edition (Java EE) application that the log or trace record relates to, if any.
requestID	Specifies the unique ID of the request that each log or trace record relates to, if any. For the application server to add the requestID extension to log and trace records, you must enable Cross Component Trace (XCT), also referred to in the administrative console as log and trace correlation. Request IDs are only added for certain types of requests, such as HTTP or JMS requests.
SIPCallId	Specifies the SIP call identifier that is being processed by the SIP proxy server or SIP container. This information is common across SIP proxy servers and SIP containers. You can use this extension to track the SIP call flow across the various components. The SIP proxy server and SIP container automatically adds this identifier to each log and trace record when HPEL logging is enabled.
SIPASId	Specifies the SIP application session ID that is being processed by the SIP container. This information is common across SIP containers. You can use this extension to track the SIP call flow. The SIP container automatically adds this identifier to each log and trace record when HPEL logging is enabled.
SIPSessionId	Specifies the SIP session ID that is being processed by the SIP container. This information is common across SIP containers. You can use this extension to track the SIP call flow. The SIP container automatically adds this identifier to each log and trace record when HPEL logging is enabled.
SIPCallId2	<p>Specifies the second SIP call ID that is associated with the same SIP application session and is being processed by the SIP container. This information is common across SIP containers. You can use this extension to track the SIP call flow. The SIP container automatically adds this identifier to each log and trace record when HPEL logging is enabled.</p> <p>If more than two SIP call IDs are associated with a single SIP application session, only the first two IDs are recorded. The additional IDs are not recorded.</p>
SIPSessionId2	<p>Specifies the second SIP session ID that is associated with the same SIP application session and is being processed by the SIP container. This information is common across SIP containers. You can use this extension to track the SIP call flow. The SIP container automatically adds this identifier to each log and trace record when HPEL logging is enabled.</p> <p>If more than two SIP session IDs are associated with a single SIP application session, only the first two IDs are recorded. The additional IDs are not recorded.</p>
thread	Specifies the thread name of the request that each log or trace record relates to.

---

# Index

## A

- administrator roles 1645
- Alpha Liberty developer tools
  - installing 1374
- Ant plug-in 1586
- APPLDATA field
  - configuring 1857
- application defined data sources 1677
- application development
  - installing 2073
- Application Monitor
  - dynamic updates 1594
- application security setting
  - restrictions 2333
- Application Server
  - creating 1424
  - installing 1374
  - logging 2313, 2319
  - runtime environments 1561
- Application Server Tools feature
  - installing 1374
- authentication
  - SPNEGO 987
- Authentication aliases 1997
- Authentication caches 1867
- Authentication configurations 1850
- authorization configurations 1939
- authorization on IBM i 1952
- authorization tasks 1939
- authorized SAFCREd resources 1857

## B

- basic authentication 2021
- basic registry security 1832
- Beta Liberty developer tools
  - installing 1374
- binding extensions 2184

## C

- client authentication
  - SSL certificates 1847, 1995
- cnfiguration elements
  - jndiEntry 2147
- command port 1437
- CommandHandler interface
  - APIs 1735
- common OSGi bundles
  - sharing 2149
- common secure interoperability version 2 1974
- communications
  - securing 1829
- Configuration Admin Service
  - persisted identity 1796
- configuration data 1796
- configuration elements
  - application-bnd 1939
  - authData 1670

- configuration elements (*continued*)
  - basicRegistry 1851, 1864
  - bundleRepository 2149
  - connectionManager 1132, 1682, 2207
  - context-root 2155, 2195, 2196, 2197, 2198, 2199, 2201, 2205
  - Embedding and Ref tags 1592
  - Embedding only 1592
  - httpSession 1610
  - interceptors 1889
  - jaasLoginContextEntry 1868
  - jaasLoginModule 1868
  - jndiReferenceEntry 2148
  - keystore 1835
  - keystores 1844
  - ldapRegistry 1852
  - ltpa 1873
  - pluginConfiguration 1604
  - quickStartSecurity 1644
  - repertoire 1847, 1995
  - scim 1859
  - security-role 1939
  - SSL 1835
  - SSLDefault 1835
  - trustAssociation 1889
  - webAppSecurity 1887, 1994
  - webContainer 1633, 1635, 1638, 1639, 1712, 1714, 1721, 1722, 1724
- configuration instances 1800
- connection pooling 1132, 1682, 2207
- connectionManager properties 1158
- context-root
  - deploying 2139
- CSIv2 1974
- custom configuration Liberty servers
  - create 1826
- Custom user registry 2015
- Custom user repository 1865

## D

- data source properties 1157
- data source types 1672
- data sources
  - restrictions
    - runtime environments 2333
- Declarative services registration 1793
- default keystores 1847, 1995
- Derby data sources migration 1159, 1161
- Design view
  - restrictions 2342
- Developer Tools
  - installing 1374
- developing password callback handler
  - WS-Security 2056
- diagnosis information 1579
- directory locations and properties 1434
- Disable MVS Console 1827
- dynamic content 1821
- dynamic updates
  - controlling 1594

## E

- EAR files
  - securing 1939
- EAR files
  - restrictions 2333
- Eclipse IDE
  - installing 1374
- Eclipse Marketplace
  - installing 1374
- Embedded server SPI 1824
- enterprise bundles
  - restrictions 2333
- entity manager
  - configuring 2157
- environment variables 1565
- Equinox OSGi console
  - administering 1555

## F

- factory configurations for default instances 1801
- feature configurations
  - features 824
- Feature definition format 1773
- feature examples
  - creating 1771
  - locating 1818
- feature FFDC records 1811
- feature logging SPI 1810
- feature restrictions
  - restrictions 2333
- feature SPIs 1771
- features installation 1823
- FFDC log files
  - logging 2313, 2319
  - restrictions 2333
- FFDC services
  - logging 2313, 2319
- FIPS support 1848

## G

- Group Database
  - securing 1946

## H

- hashtable login module 2002
- HTTP access log 2289
- HTTP authentications
  - Trust Association Interceptors 1889
- HTTP client properties 2182
- HTTP port
  - configuring 1556, 1870
- HTTP servlets
  - features 826
- httpEndpoint SSL configuration 1850

- HTTPS listener
  - features 826
- HTTPS port
  - features 826
  - restrictions 2333

## I

- ID attributes
  - configuring 1857
- Identity assertion customization 2013
- include statements 1588
- installation integrity 1415
- installation procedure
  - installing 1374
- IP addresses
  - bootstrap properties 1437

## J

- JAAS authentications
  - login modules 1868
- JAAS custom login modules
  - developing 2002
- Java command
  - administering 1731, 1734
  - configuration variables 1590
- JAVAENV DD statements
  - administering 1731, 1734
- JavaMail
  - Administering 1730
- JAX-RS
  - context objects 2175
  - secure downstream resources 2165
- JAX-RS 2.0 2162, 2175
- JAX-RS applications
  - deploying 2159
- JAX-WS applications
  - deploying 2178
- JDBC applications
  - deploying 2150
- JDBC data source
  - restrictions
    - runtime environments 2333
- JDBC data source
  - restrictions
    - tools 2342
- JDBC driver configurations 1157
- JDBC driver location
  - deploying 2150
- JDBC drivers
  - deploying 2150
- JDBC tracing options 2152
- JDBC vendor properties 1672
- JMX connectors 1641, 1642, 1645, 1993
- JMX MBeans 1647
- JNDI binding 1819
- JNDI binding for constants 2147
- JNDI binding for dynamic values 2148
- JPA annotations
  - restrictions 2333
- JPA applications
  - configuring 2157
- JSF framework
  - features 826

- JSF support
  - restrictions 2333
- JVM monitoring 2267
- JVM options
  - bootstrap properties 1437
- JVM start options
  - process types 1019

## L

- LDAP registry
  - configuring 1857
- Liberty 1401, 2162, 2175
  - installing 1374
  - OSGi console 1587
  - passwords 1858, 1941
  - restrictions 2333
- Liberty
  - administering 1555
  - OSGi console 1587
- Liberty code
  - process types 1019
- Liberty feature project
  - specifying API and SPI packages 1784
- Liberty feature projects
  - adding OSGi bundles 1784
  - creating 1783
- Liberty features 1783, 1784
  - installing 1785, 1786
- Liberty features
  - administering 1587
  - deploying 2150
- Liberty profile
  - adding 2141
  - development environments 2073
  - global handlers 1812
  - monitoring local files 1809
  - process types 1019
- Liberty Profile
  - creating 1424
  - exploring 1561
- Liberty runtime environment
  - overview 1, 1553
  - process types 1019
- Liberty server
  - administering 1731, 1734
  - dumping 1579
  - packaging 1581, 2144
- Linux shell
  - overview 1
- Local download
  - creating 1424
- local JMX connectors 1642
- Location services 1809
- log files
  - restrictions 2333
- logging configuration 2313, 2319
- LTPA keys 1873

## M

- MBeans attributes and operations 1654
- Merged Configuration view
  - configuring 1562

- merged view
  - configuring 1562
- migrating CXF WS-Security 2067
- MVS console 1

## O

- OAuth tasks 1954
- optimized local adapters
  - administering 1697
  - development 1949, 2073
  - environment enablement 1697, 1703
  - planning
    - z/OS 1688
    - z/OS 1690
- OSGi applications 1600
  - deploying 2149
  - features 826
  - OSGi application integration 2134
- OSGi applications
  - deploying 2139
  - development environments 2073
  - overview 1
  - running 2141
  - runtime environments 2333
- OSGi blueprint container specification
  - features 826
- OSGi bundles
  - adding to a Liberty feature
    - project 1784
    - simple activation 1788
- OSGi Configuration Admin specification
  - persisted identities 1796
- OSGi console
  - administering 1555
  - using 1587
- OSGi console port
  - using 1587
- OSGi metatype service extensions 1801
- OSGi Metatype Service specification
  - configuration metatypes 1798
- OSGi services availability 1792
- OSGi services registration 1789, 1790
- OSGi tool
  - installing 1374

## P

- password encryption
  - encoding 1844
- plugin-cfg.xml in Liberty 1604
- Port numbers
  - Default port numbers 1440
- product extensions
  - features 968
- Project Explorer view
  - creating 1424
- protected features 1816

## R

- REALM class
  - configuring 1857
- reference tags 1592
- role-based authorization 1939

- ROOT variable
  - administering 1731, 1734
- runtime environments
  - creating 1424
  - exploring 1561
- Runtime Explorer
  - exploring 1561

**S**

- SAF product
  - configuring 1857
- SAF registry
  - features 826
- SAF registry
  - overview 1
- SAF registry service
  - configuring 1857
- SAFCRED resource
  - configuring 1857
- Schema Reference
  - server configurations 1563
- SDBM alternative setup
  - passwords 1858, 1941
- secure communications 1833, 1974
- secure Web services
  - communication 2018
- securing tasks 2058
- Security 2070
- Security differences 1008
- security features 1829
- security infrastructure extensions 1998
- Security Server
  - passwords 1858, 1941
- securityUtility command 1844
- SERVER class
  - configuring 1857
- Server Configuration editor
  - displaying 1562
- server configuration files
  - logging 2313, 2319
- server configurations
  - include statements 1588
- server configurations
  - configuring 1556, 1870
  - creating 1424
  - displaying 1562
  - logging 2313, 2319
  - schema 1563
- Server page 1424
- server ports 1437
- SERVER profile
  - administering 1731, 1734
  - configuring 1942, 1943
- Server Version
  - logging 2313, 2319
- Servers view
  - configuring 2141
  - creating 1424
  - editing 1556
  - exploring 1561
  - restrictions 2342
  - schema 1563

- Servers view (*continued*)
  - server configurations 1562
- serving environment
  - installing 1374
- servlets loading 1633, 1635, 1638, 1639, 1712, 1714
- session failover 1610
- Session Initiation Protocol (SIP)
  - Administering 1728
  - Deploying SIP applications 2156
  - Developing 2131
  - Troubleshooting 2353
- shared state variables 2002
- single sign-on
  - HTTP requests 987
  - LTPA cookies 1887, 1994
- SIP 1033
  - application composition 1035
  - Asynchronous API 2130
  - classes 2133, 2134
  - compliance 1036
  - container 1035
  - development 2126
    - Asynchronous Invocation API 2128
    - PRACK 2126
  - headers 2132
  - JSR 289 1034
  - routers 1035
  - SIP applications 1033
  - SIP servlet 1033, 1034
  - troubleshooting 2349
- SSL certificate
  - creating 1844
- SSL certificates 1844
  - features 826
- SSL communications 1834, 1888, 2019, 2024
- SSL configuration attributes 1835
- STARTED profile
  - administering 1731, 1734
  - configuring 1942, 1943
  - process types 1019
- Supplementary Group IDs
  - unauthorized services 1946
- syncToOSThread for applications 1739
- syncToOSThread for J2C
  - connections 1740

**T**

- TAI configuration 1891
- TAI customization 1998
- TAI user feature 1820
- third-party features development 1771
- Thread pool monitoring 2269
- Tools
  - installing 1374
- Tools feature
  - installing 1374
- Transaction logs 1670
- transaction recovery 1669, 1670

- transaction service
  - administering 1669
- Troubshooter reference
  - abend 2347
  - messages 2344
- Trust Association Interceptors 1889

**U**

- unauthorized services
  - SAF registry 1946
- usable callbacks 2002
- user custom properties 2182
- user ID
  - administering 1731, 1734
  - configuring 1942, 1943
  - restrictions 2333
- UserRegistry service 1857

**V**

- vendor databases configuration 1672

**W**

- Web application monitoring 2268, 2286, 2287, 2288
- Web applications
  - features 826
- web applications
  - restrictions 2333
- web services applications
  - deploying 2159
- web services binding 2179
- Web services monitoring 1860, 2270
- WebSphere Application Server Liberty profile 1561
- WebSphere Runtime Environment page
  - creating 1424
- WebSphere Server page
  - creating 1424

**X**

- XMI files
  - securing 1939
- XMI files
  - restrictions 2333
- XML code
  - persisted identities 1796
- XML configuration files
  - bootstrap properties 1437
- XML files
  - basic architecture 6
  - configuration metadata 1798
  - Liberty Repository 965
  - localizing 1807
  - server configurations 21, 1767, 1768
- XML snippets
  - features 1587